Security zSecure Admin and Audit for RACF
Version 1.13

User Reference Manual

LC14-7663-00

Security zSecure Admin and Audit for RACF
Version 1.13

User Reference Manual

LC14-7663-00

Note
Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 1697.

November 2011

This edition applies to version 1, release 13, modification 0 of IBM Security zSecure Admin (product number 5655-T01), version 1, release 13, modification 0 of IBM Security zSecure Audit for RACF (product number 5655-T02), IBM Security zSecure Alert (product number 5655-T11), IBM Security zSecure Visual (product number 5655-T09), IBM Tivoli Compliance Insight Manager Enabler for z/OS (product number 5655-T15) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This manual provides information about IBM Security zSecure Admin and Audit for RACF including:

- A guide describing how to use the product features from ISPF panels.
- RACF® administration and audit user documentation.
- Both general and advanced user reference material for the CARLa command language, the CKGRACF command language, and the SELECT/LIST fields.
- Instructions for installing and using zSecure Collect.

Intended audience

This publication is intended for systems programmers and administrators responsible for installing, configuring and monitoring security for RACF. Readers must be familiar with RACF concepts and commands.

What this publication contains

This manual describes zSecure running on a z/OS® platform. For information on running on the z/VM® platform, see the *IBM Tivoli zSecure Manager for RACF z/VM: User Reference Manual*.

This publication refers to the *IBM® Security Server, RACF component* as RACF.

In this publication, sections that include the word *Guide* in the title provide detailed information about using the product through an ISPF interface. These sections also provide some background information on RACF. The other sections of the manual contain reference material for more advanced users. The manual is written with the assumption that readers have a working knowledge of ISPF and RACF . You can also refer to the *IBM Security zSecure Admin and Audit for RACF: Getting Started Guide* for a tutorial and examples on the basic product functionality.

The following items are discussed in this manual:

- Chapter 1, "Introduction," on page 1 provides an overview of the product architecture and introduces the main menu options and line commands available through the zSecure ISPF interface.
- Chapter 2, "RACF Administration Guide," on page 51 introduces the functions available from the RA RACF Administration menu as well as the help desk functions.
- Chapter 3, "RACF Audit Guide," on page 255 explains how to use the zSecure Audit functions available from the AU Audit menu. Information includes instructions for migrating from the Data Security Monitor (DSMON) program to zSecure, auditing RACF security options and tables, RACF user, resource profiles, and CKGRACF, instructions on using zSecure to identify inconsistencies in the RACF database and to resolve common RACF problems. The chapter also provides an overview of sample audit reports that can be customized using CARLa Auditing and Reporting Language (CARLa).
- Chapter 4, "Resource reports," on page 383 describes the display and reporting options for RACF resources. There are dedicated options for reporting on TCP/IP configurations, z/OS UNIX, CICS, IMS, and DB2.

- Chapter 5, “System Audit Guide,” on page 425 explains the most important standard system reports. Both ISPF and batch reports are covered in this chapter.
- Chapter 6, “Library Audit Guide,” on page 529 discusses the library update report used to find and display changes to members of partitioned data sets.
- Chapter 7, “SMF and HTTP Reporting (Events menu),” on page 545 explains how to use zSecure for SMF processing and describes the SMF reports, which can be used to monitor user activity and MVS™ events. This chapter also provides additional information on unloading and selecting security data sets.
- Chapter 8, “RACF Offline,” on page 593 describes how to use the RACF Offline component to issue most RACF commands against an inactive RACF database.
- Chapter 9, “Merge Usage Guide,” on page 623 explains how the MERGE commands work and how to use them to compare and synchronize RACF databases.
- Chapter 10, “RACF Access Monitor,” on page 643 describes the Access Monitor program and explains how RACF administrators can use it to cleanup the RACF database. It also explains how the program can be used to evaluate the effects of changes to the RACF database before putting them into production.
- Chapter 11, “Calling zSecure,” on page 689 provides a detailed reference on how to use zSecure in batch mode. This section also provides information on unloading and selecting security data sets in this chapter.
- Chapter 12, “CARLa Command Language,” on page 713 is the reference chapter for the CARLa Auditing and Reporting Language (CARLa) for creating your own reports, to customize standard reports, or to perform certain actions such as making an unload file of the security databases.
- Chapter 13, “SELECT/LIST Fields,” on page 953 lists the fields you can use to generate reports.
- Chapter 14, “CKGRACF Command Language,” on page 1499 is the reference chapter for CKGRACF commands. CKGRACF allows a central security administrator to provide specific access rights to a local administrator. This ability means that local administrators do not need group special privileges which would probably allow them too much control over the security database. In addition, security administrators can make the divisions between authority levels more flexible.
- Chapter 15, “Problem Determination Guide,” on page 1573 discusses the most common problems and their solutions.
- Chapter 16, “zSecure Collect for z/OS,” on page 1591 discusses the zSecure Collect program that collects data on the connections in your I/O subsystem, as well as information on the way your z/OS system is configured.
- Chapter 17, “Setup and Library Commands,” on page 1641 describes how to set up and customize zSecure.

For information on zSecure messages and return codes refer to *IBM Security zSecure: Messages Guide*.

For information on product installation, security setup, and customization for all users at the same time, refer to *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Publications

This section lists publications in the IBM Security zSecure library, prerequisite publications, and related IBM publications. It also describes how to access and order publications online.

Note: You can find information about the zSecure products for z/OS systems at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.13/welcome.htm.

IBM Security zSecure library

The following documents are available in the IBM Security zSecure library:

- *IBM Security zSecure: Release Information*

  For each product release, the Release Information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. Access the current version of the release information from the IBM Security zSecure Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

- *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*, SC14-7662-00

  Provides information about installing and configuring the following IBM Security zSecure components:

  – IBM Security zSecure Admin
  – IBM Security zSecure Audit for RACF, ACF2 and Top Secret
  – IBM Security zSecure Alert for RACF and ACF2
  – IBM Security zSecure Visual for RACF
  – IBM Tivoli Compliance Insight Manager Enabler for z/OS

- *IBM Security zSecure Admin and Audit for RACF: Getting Started Guide*, GI11-9162-00

  Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.

- *IBM Security zSecure Admin and Audit for RACF: User Reference Manual*, LC14-7663-00

  Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the features from ISPF panels, RACF administration and audit user documentation with both general and advanced user reference material for the CARLa command language and the SELECT/LIST fields. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2: User Reference Manual*, LC14-7664-00

  Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information including message and return code lists, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2: Getting Started Guide*, GI11-9163-00

  Describes the IBM Security zSecure Audit for ACF2 product features and provides user instructions for performing standard tasks and procedures such as

analyzing Logon IDs, Rules, and Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.

- *IBM Security zSecure Audit for Top Secret: User Reference Manual*, LC14-7665-00

  Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.

- *IBM Security zSecure Alert: User Reference Manual*, SC14-7666-00

  Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2.

- *IBM Security zSecure Visual: Client Manual*, SC14-7669-00

  Explains how to set up and use the IBM Security zSecure Visual Client to perform RACF administrative tasks from the Windows-based GUI.

- *IBM Security zSecure Command Verifier: User Guide*, SC14-7670-00

  Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.

- *IBM Security zSecure CICS Toolkit: User Guide*, SC14-7671-00

  Explains how to install and use IBM Security zSecure CICS Toolkit to provide RACF administration capabilities from the CICS® environment.

- *IBM Security zSecure: Messages Guide*, SC14-7667-00

  Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

- *IBM Security zSecure: Quick Reference*, SC14-7668-00

  This booklet summarizes the commands and parameters for the following IBM Security zSecure suite components: Admin, Audit, Alert, Collect, and Command Verifier. Obsolete commands are omitted.

- *IBM Security zSecure: Documentation CD*, LCD7-1387-09

  Supplies the IBM Security zSecure Information Center, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is only available to licensed users.

- *Program Directory: IBM Security zSecure Suite CARLa-driven components*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of zSecure CARLa-driven components: Admin, Audit, Visual, Alert, and the IBM Tivoli Compliance Insight Manager Enabler for z/OS. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

- *Program Directory: IBM Security zSecure CICS Toolkit*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CICS Toolkit. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center

available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

- *Program Directory: IBM Security zSecure Command Verifier*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure Command Verifier. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

- *Program Directory: IBM Security zSecure Admin RACF Offline*

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM Security zSecure Admin RACF Offline component of IBM Security zSecure Admin. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure Information center available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_1.13/welcome.html.

Related z/OS documentation

More information about RACF and the types of events that can be reported using zSecure Admin and Audit can be found in several IBM manuals. Information about the various types of events that are recorded by RACF can be found in the *RACF Auditor's Guide*. To access manuals in the z/OS online library, enter order numbers at the following URL: http://www-03.ibm.com/systems/z/os/zos/bkserv/.

Table 1. z/OS manuals in z/OS online library

Manual title	Order number
z/OS Security Server RACF Command Language Reference	SA22-7687
z/OS Security Server RACF Security Administrator's Guide	SA22-7683
z/OS Security Server RACF Auditor's Guide	SA22-7684
z/OS Security Server RACF System Programmer's Guide	SA22-7681
z/OS Communications Server IP Configuration Reference	SC31-8776
z/Architecture® Principles of Operation	SA22–7832

Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli® products, as they become available and whenever they are updated, to the Tivoli Information Center website at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on paper that is not letter-size, set the print option that Adobe Reader uses to print letter-size pages on paper that is not letter-size.

Ordering publications

You can order many Tivoli publications online at:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Select http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Licensed publications: IBM Security zSecure licensed publications have a publication number that starts with an *L* , such as LC27-2781-00. To request a licensed publication, send an email to:

tivzos@us.ibm.com

. In the email include your IBM customer number, list of publication numbers, and your contact information. IBM contacts customers to complete orders. To contact IBM, see “Support for problem solving” on page xviii.

Accessibility

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use software products successfully. For keyboard access in the zSecure products, standard shortcut and accelerator keys are used by the product, where applicable, and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Visit the IBM Accessibility Center at http://www.ibm.com/alphaworks/topics/accessibility/ for more information about IBM's commitment to accessibility.

Tivoli technical training

For Tivoli technical training information, access the IBM Tivoli Education website at http://www.ibm.com/software/tivoli/education

.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from experienced Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the Tivoli Users Group at http://www.tivoli-ug.org.

Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Navigate to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, navigate to http://www.ibm.com/software/support/isa.

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**).
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, directory names, and path names
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Chapter 1. Introduction

zSecure provides cost-effective security administration, improves service by detecting threats, and reduces risk with automated audit and compliance reporting. The product does this by increasing the functionality of your security system and reducing processing time. The clear structure and the possibility to make a more granular division between administration authority levels enable you to distribute the workload without compromising security.

zSecure runs on a z/OS or z/VM platform and uses RACF information and functionality.

Note: For an overview of the User Reference Manual content and other zSecure documentation, see "What this publication contains" on page xi.

General information

To better understand the zSecure products, it helps to have an overview of the program structure. The primary processing programs are large modules that can be used in batch or interactive mode. Interactive mode is most common, although batch mode can be useful for automated, periodic checks or for producing daily reports.

zSecure provides an interactive user interface implemented in ISPF using the *panel, skeleton* and *message* libraries supplied with zSecure. ISPF is the main program running during an interactive session, calling the zSecure application program as needed.Figure 1 on page 2 illustrates the general flow. The user completes tasks through ISPF panels, which generate commands that are sent to zSecure. These commands generate the RACF commands to alter the user ID as requested.

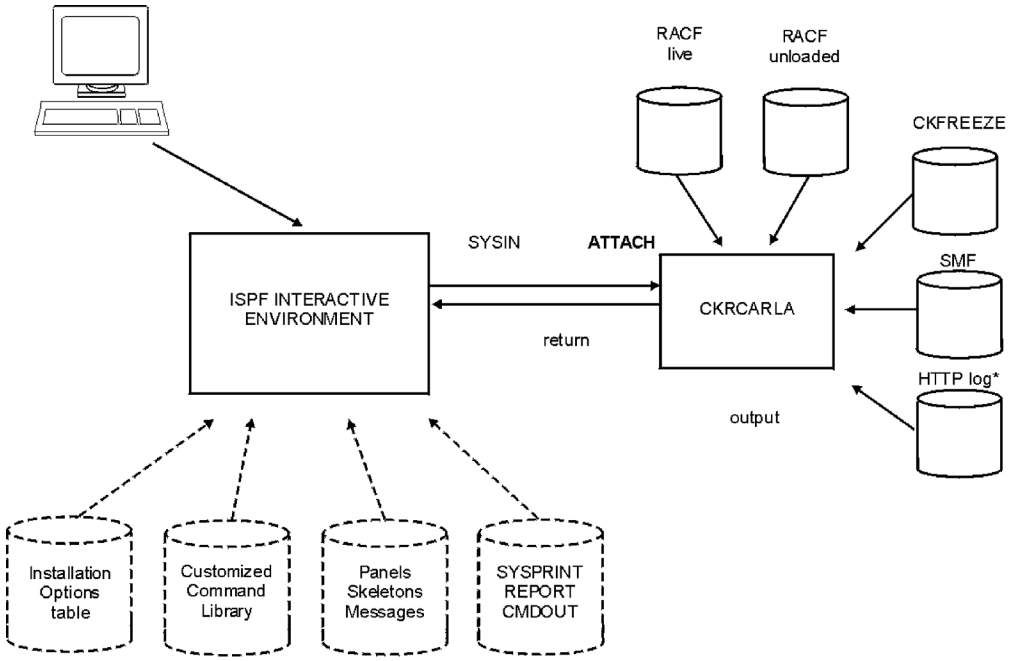


Figure 1. Conceptual Data flow

This general design with separate interactive and noninteractive components provides a number of practical advantages:

- It separates interactive interfaces from the application program. This separation allows more flexibility in designing and using the interfaces and programs, especially when customizing the ISPF interface.
- Any functions that can run interactively can also run in batch mode.
- An installation can create customized reports using the CARLa Auditing and Reporting Language (CARLa) program and run these reports from the ISPF panels or in batch.

zSecure is command driven using the CARLa program which is described in this manual. A typical user who runs zSecure from the ISPF user interface does not need to know the CARLa language because the code is automatically generated from the settings and selections specified on the product panels.

Because the standard, predefined zSecure reports are comprehensive, customized reports might not be required. However, you can customize the reports if necessary. Using zSecure in batch provides advantages from a security monitoring function. For example, you can set up a batch job to automatically run a set of zSecure checks and reports every day or every week rather than having a user set up and run the reports manually from the ISPF interface.

A comprehensive set of sample reports is available in a data set referred to as the CARLa library (ddname `CKRCARLA`, data set `SCKRCARL`).

Tip: See Chapter 11, “Calling zSecure,” on page 689 for a list of available CARLa scripts.

Data Sources

zSecure uses the following types of data and sources of data:

- Data from your security system which can be obtained from the local system and remote systems.
- Data which describes your system configuration (control blocks and DASD)
- Data describing events on your system (SMF)

The following figure shows the zSecure data input sources and data flow.

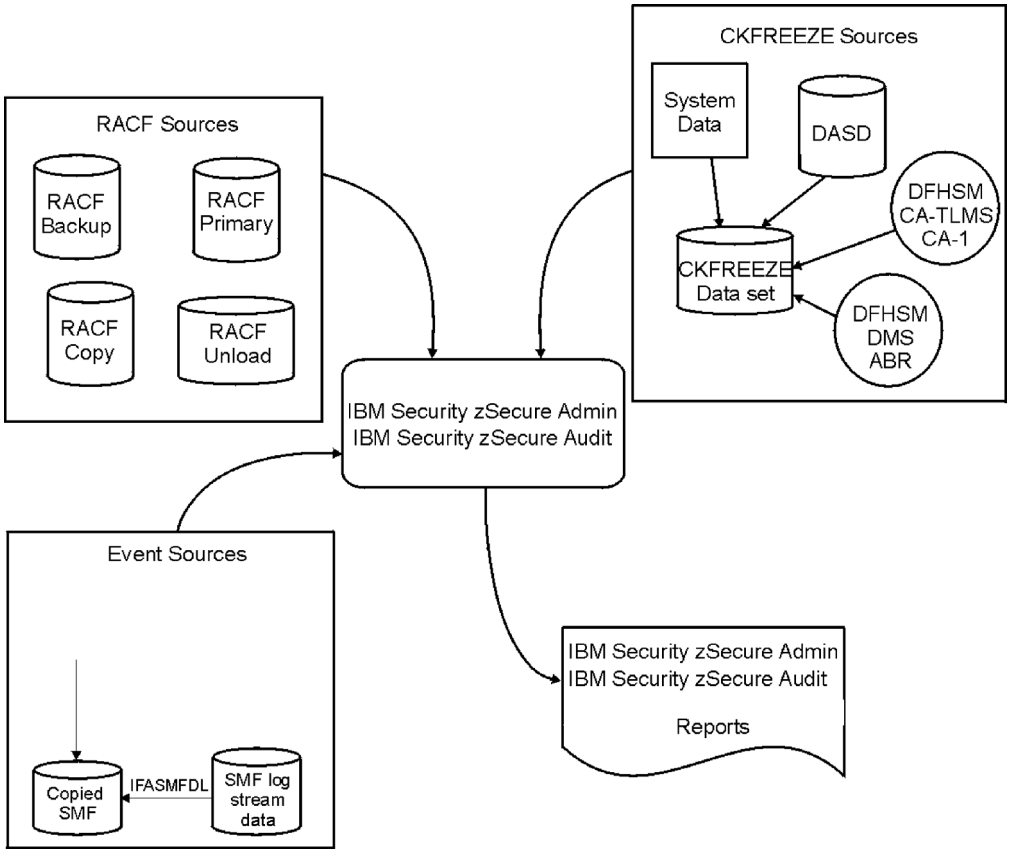


Figure 2. zSecure Input Sources

You define input sets that specify the data sources for zSecure from the "SE.1 Setup - Input files" on page 1645 menu option. For example, one input set might only contain the live security database. Another set might contain the live security database combined with a file containing system configuration data. Another set might use unloaded security data, system configuration data, and several SMF files. During a zSecure session, you can switch between input sets with the `SETUP` functions.

Data from your security system

zSecure usually requires RACF data that can come from four sources:

- Primary live RACF database
- Backup live RACF database
- Unloaded RACF data
- A copy of a RACF database, or an active RACF database from another system.

Note: zSecure creates an unloaded copy of RACF data by reading the live RACF database and creating a copy in a proprietary format suitable for high-speed

searches. The zSecure process is much faster and uses much less space than the RACF database unload program IRRDBU00.

You can use zSecure for the administration and auditing of profiles, resources, and settings from multiple systems. Beginning with zSecure release V1.12, you can configure the input data sources for systems of interest to collect the information directly from each system. The data sets can then be used through the ISPF interface or in a CKRCARLa program.

In addition to multisystem reporting, the product also supports routing commands to a remote system using zSecure services or existing RACF Remote Sharing Facility (RRSF) services. zSecure provides the following command routing options: Route to the local system, or route to a remote system using NJE batch jobs, RRSF services, or zSecure services. For additional information about command routing options, see "Using remote data."

Note: Support for working with data obtained directly from remote systems and remote command routing using either zSecure services or RRSF services is available beginning with zSecure V1.12. To use these functions, the zSecure Server component must be installed, configured, and activated. See *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

If you are using zSecure V1.11 or earlier, you can still report on data from multiple systems. However, you cannot obtain the information directly from a remote system. Instead, you must transfer the data sets containing information obtained from each system to a central system. Then, those copied data sets can be used as input to the CKRCARLA program, or as input files in the ISPF User Interface using the `SETUP FILES` function.

Using remote data

Beginning with V1.12, zSecure Admin and zSecure Audit support the use of remote data sets as input for creating reports and displays. This functionality is called multisystem support because it enables reporting and managing multiple systems from a single session. This function is also integrated with zSecure Admin support for routing RACF commands using zSecure services or RRSF services. Access to this functionality requires that the zSecure Server is installed.

Using zSecure services for remote data access requires the zSecure Server which runs in a separate server address space. The zSecure Server performs the necessary functions for command routing and communicating with remote systems to access RACF databases, SMF input files, CKFREEZE data sets, and other defined data sets. These functions only support input files from remote systems. Output files for the generated report data must be allocated on the local system.

For more information, see the following topics:

- "Reporting on data from remote systems"
- "Command routing" on page 5

Reporting on data from remote systems: Using remote data for creating reports is useful for ad-hoc reporting about profiles or settings. Because accessing large amounts of remote data is slower than accessing the same data locally, remote data access is less suited for queries that require processing of the entire security database or the entire `CKFREEZE` data set. If your query specifies a remote data source but does not specify a CKFREEZE data set with the same remote specification, a `CKFREEZE` data set describing the active configuration of the remote system is added automatically.

Using remote data for creating reports is useful for ad-hoc reporting about records or settings. Because accessing large amounts of remote data is slower than accessing the same data locally, remote data access is less suited for queries that require processing of the large quantities of data like the entire `CKFREEZE` data set. If your query specifies a remote data source but does not specify a CKFREEZE data set with the same remote specification, a `CKFREEZE` data set describing the active configuration of the remote system is added automatically.

You can specify the location of an input data source on a remote system using the `SETUP FILES` interface in the ISPF environment or the CARLa `ALLOCATE` statement. See Chapter 17, "Setup and Library Commands," on page 1641 and "ALLOCATE" on page 718.

Using remote data requires the following authorizations:

- Access to the remote destination.
- Access to the remote data set using the zSecure Server.
- For all data sets other than the live data sources, authorization to access the data set.

These authorizations must be established before you can access the remote data. The resources and profiles required for setting up these authorizations are described in *Setting up security for zSecure* in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. Contact your system administrator for additional information and assistance.

Command routing: When you are issuing commands that are generated by CKRCARLA, you can select how the commands are routed:

- Routing to the local system.
- Routing using zSecure services.
- Routing using RRSF services.
- Routing through NJE batch jobs.

You can also select if you want to specify the command routing for each and every command, or if you want to use default routing. If no explicit command routing is specified, commands are sent to the local system. For more information about command routing, see "SE.4 Setup - Confirm" on page 1655.

The authorizations required for command routing depend on the routing method specified:

- Routing using zSecure services requires authorization to the appropriate zSecure resources.
- Routing using RRSF services requires an approved user association The required RRSF authorizations are described in the *RACF Security Administrator's Guide* and the *RACF Command Language Reference*
- Routing through NJE batch jobs requires authorization to route jobs to the remote system.

These authorizations must be established before you can route commands to remote systems. The resources and profiles required for setting up these authorizations are described in *Setting up security for zSecure* in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. Contact your system administrator for additional information and assistance.

Data describing your system configuration (control blocks and DASD)

zSecure uses z/OS control block data and DASD data. These data are read from a CKFREEZE data set, created by zSecure Collect. “SE.2 Setup - New files” on page 1653 explains how to create a CKFREEZE data set. zSecure Collect uses APF-authorized functions to retrieve data from other address spaces and from read-protected common storage. zSecure Collect also reads all online VTOCs, VVDSes, catalogs, selected PDS and PDSE directories, UNIX file systems, and optionally calculates digital signatures at the member and data set level when requested. Additionally, batch collection permits you to analyze a remote system where the data was collected.

Data describing events on your system (SMF)

The SMF data can come from live SMF data sets, SMF log streams, or from sequential SMF data sets produced with the IFASMFDP or IFASMFDL programs. The IFASMFDP or IFASMFDL programs are provided by IBM to unload SMF records from the live SMF data sets and SMF log streams respectively. These sequential files can be on disk or tape, although many installations might not permit TSO users to mount tapes for interactive use. zSecure cannot process pseudo-SMF files created by the RACF REPORT WRITER or by the IRRADU00 SMF unload program.

zSecure User roles

zSecure provides functionality for different types of users. In this documentation, the following titles describe the different user roles. These descriptions are provided to clarify the zSecure specification of these roles in case your organization has different titles or descriptions for a task.

Central Security Administrators
The employees who are responsible for the system-wide administration of the mainframe security systems. They have extensive knowledge of security administration and of the mainframe environment. These people are responsible for creating and, possibly, implementing the company standards.

System Programmers
People involved with the running of the mainframe environment. If they are also involved with the security they probably have the same detail level of knowledge as central security administrators.

Decentralized / local Administrators
Technical people on local or decentralized level with a fair knowledge about the mainframe security systems. They are responsible for the proper running of the security systems at their level or department. They work within the settings made by the centralized administrator but might have great freedom within these settings.

Auditors
People with a good knowledge about security matters but not necessarily about the technical part of the security systems. They audit the system and report to the administrators.

Local Security Administrators
Local Security Administrators such as help desk employees are responsible for administrative task such as resetting passwords, copying users, and so on.

The IBM Security zSecure products

IBM Security zSecure suite is a group of products that improves the efficiency and maintainability of your mainframe security environment. The main products are zSecure Admin and zSecure Audit. These products can be used separately or in combination with the other zSecure products.

The following descriptions are intended to provide a brief overview of the products. More detailed information about zSecure Admin and Audit is available from other topics in this documentation. For additional information about any of the other zSecure products, refer to the documentation for those products.

zSecure Admin
Provides a user-friendly layer in the form of an ISPF interface on top of RACF and extends the functionality so users can enter and process administrative commands more quickly, generate custom reports, and thoroughly clean up security databases. zSecure Admin also provides administrative authority in a more granular fashion so people only have the specific amount of administrative authority required for their job.

zSecure Audit
Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures. It provides standard and customized reports that warn of policy exceptions or violations. This component is available for RACF, ACF2, and Top Secret.

zSecure Alert
Mainframe audit solution that enables you to detect and report security events and exposures on z/OS systems protected with RACF or ACF2 that issues alerts for important events relevant for the security of the system at the time they occur.

zSecure Visual
zSecure Visual is comprised of two components: a client and a server. zSecure Visual client is a Windows-based graphical user interface for RACF administration. zSecure Visual server establishes a secure connection directly with RACF to enable decentralized administration from a Windows® environment.

Tivoli Compliance Insight Manager Enabler for z/OS
IBM Tivoli Compliance Insight Manager Enabler for z/OS is an optional component. You can use it to connect the mainframe to the cross-platform auditing and compliance solution IBM Tivoli Compliance Insight Manager or Tivoli Security Information and Event Manager. When this option is configured, mainframe events and alerts can be managed centrally from an enterprise compliance dashboard for reporting across applications, databases and operating systems.

zSecure Command Verifier
Mainframe policy enforcement solution that adds granular controls for RACF to help prevent errors and noncompliant commands. This product runs in the background to verify your RACF commands against company policies and procedures. If the command does not comply with the policy, it is blocked or fixed. It can run independently from the other zSecure components.

zSecure CICS Toolkit
Enables most RACF administration activities from a CICS environment which can be used instead of TSO.

zSecure Manager for RACF z/VM
Simplifies the process of managing mainframe security and enables you to quickly identify and fix problems in RACF on z/VM. zSecure Manager for RACF z/VM automates recurring and time-consuming security tasks.

Note:

This manual only provides documentation for zSecure Admin and Audit for RACF. For information about other zSecure products, see "IBM Security zSecure library" on page xiii.

zSecure key programs

The following descriptions are intended to provide a brief overview of programs that provide key functionality within the IBM Security zSecure products. More detailed information about programs for zSecure Admin and Audit is available from other topics in this user documentation. For additional information about zSecure Visual or any of the other zSecure products, see the documentation for those products.

C2PACMON
The `C2PACMON` program is the main program for the Access Monitor for RACF monitor which provides RACF administrators with the data required to remove unused or obsolete resource profiles and authorizations defined within profiles. This function is used for RACF database cleanup. The Access Monitor also allows RACF administrators and analysts to run simulations against a candidate RACF database to test resource profiles and the access rights defined within them.

C2POLICE
This program is the main program of the zSecure Alert address space. It intercepts SMF records and WTO messages to detect events that require alerts to be sent out to system operators, security administrators and/or security personnel via for instance EMAIL or SMS messages.

CKGRACF
The `CKGRACF` program is part of zSecure Admin. It is used for handling Queued commands (like temporary access), revoke or resume schedules, User data fields and various other functions that require updating RACF profiles. This program is also used by zSecure Visual.

CKNSERVE
The `CKNSERVE` program is the main program for the zSecure Server which performs the necessary functions for communicating with remote systems to route commands and access RACF databases, SMF input files, `CKFREEZE` data sets, and other defined data sets. For more information, see "Using remote data" on page 4.

CKRCARLA
The CKRCARLA program is the main program used in zSecure products. Using the special purpose CARLa Auditing and Reporting Language (CARLa), the CKRCARLA program processes SMF, CKFREEZE data, and other types of information. The program is used by the following zSecure products: Admin, Audit, Alert, Visual, and the Tivoli Compliance Insight Manager Enabler for z/OS.

zSecure RACF Exit Activator
The zSecure RACF Exit Activator, `C2XACTV` provides dynamic exit support for some RACF exits. The main purpose of the RACF Exit Activator program is to

install exits required by various zSecure products. This program supports the following products: IBM Security zSecure Admin and Audit, and Alert and Tivoli Compliance Insight Manager Enabler for z/OS. For additional information about the program, see Chapter 11, "Calling zSecure," on page 689. For details on installing the zSecure RACF Exit Activator program, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

RACF Offline
IBM Security zSecure Admin provides the RACF Offline function to allow you to execute and test RACF commands on a RACF database that is not active in the system. Using this program, you can test changes to RACF definitions without impacting any other software executing on the system and without using a dedicated test system.

zSecure Collect
The zSecure Collect program, `CKFCOLL` gathers information about your z/OS system configuration. Designed to collect data quickly using minimal system resources, this program does not provide any reporting functions other than some messages and a summary report. Analysis of the collected data is done by the CKRCARLA program. For more information, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

Starting the interactive component

Typically, users complete zSecure work from the zSecure user interface. The user interface is implemented using an ISPF application available under TSO on z/OS. Depending on how the system administrator has configured the product, you can start zSecure by selecting the option from a menu or by entering a custom command. Ask your system administrator for instructions.

If the zSecure was installed using the default configuration and settings, the product can be started from TSO on z/OS under ISPF by using the implicit TSO EXEC command. That is, you can start zSecure by typing the following command on any ISPF command line:

```
TSO CKR
```

After this, the primary option menu is displayed.

Note: You can run multiple instances of zSecure in ISPF split-screen mode provided that all zSecure instances are the same version.

Other methods to invoke zSecure, including in batch and through TSO line mode commands, are described in Chapter 11, "Calling zSecure," on page 689.

Panel structure

When you start an interactive zSecure session the **main menu** is shown. This **main menu** contains an overview of the available options. Exactly which options are displayed depends on several factors. Options that are disabled or not installed are not shown. Options for which you do not have enough authorization are not shown. Moreover, your system administrator can remove or rename some options.

The initial look of the **Main menu** is shown in the following figure.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                      zSecure Admin+Audit - Main menu
Option ===> ____________________________________________________________

 SE   Setup           Options and input data sets
 RA   RACF            RACF Administration
 AU   Audit           Audit security and system resources
 RE   Resource        Resource reports
 AM   Access          RACF Access Monitor
 EV   Events          Event reporting from SMF and other logs
 CO   Commands        Run commands from library
 IN   Information     Information and documentation
 LO   Local           Locally defined options
 X    Exit            Exit this panel

Input complex: Active primary RACF data base
```

Figure 3. Security zSecure main menu on entry

The options on this panel are called *primary* options. Some options expand when you select them. Figure 4 shows a sample of the expanded main menu. Notice that the primary options are still available.

```
    Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
       zSecure Admin+Audit for RACF - Main menu
Option ===> ____________________________________________________________

                                                                More:     +
 SE   Setup           Options and input data sets
 RA   RACF            RACF Administration
   U    User            User information
   G    Group           Group information
   D    Data set        Data set profiles
   R    Resource        General resource profiles
   S    Settings        Setropts and class settings
   H    Helpdesk        One-panel helpdesk options
   Q    Quick admin     Quick User Administration
   1    Access          Access Check
   2    Queued          Display and action on profiles with QUEUED commands
   3    Reports         Reports with profiles and resources
   4    Mass update     Specify mass copy/recreate/delete actions
   5    DIGTCERT        Work with digital certificates
   C    Custom          Custom report
 AU   Audit           Audit security and system resources
 RE   Resource        Resource reports
 AM   Access          RACF Access Monitor
 EV   Events          Event reporting from SMF and other logs
```

Figure 4. zSecure main menu after selecting option RA

Using the UP- and DOWN-keys shows the rest of the menu.

Security zSecure remembers the last menu option you expanded. When you start a new session, the session starts with that menu option expanded.

Additional information about using the panels is available in “A sample run” on page 17. Table 2 provides an index to the documentation for the Menu options. See “IN INFORMATION - Information and documentation” on page 35 for additional documentation overview information.

Table 2. Documentation references for zSecure Menu options

Menu option	Documentation reference
SE Setup	Chapter 17, “Setup and Library Commands,” on page 1641
RA RACF	Chapter 2, “RACF Administration Guide,” on page 51
AU Audit	Chapter 5, “System Audit Guide,” on page 425
RE Resources	Chapter 4, “Resource reports,” on page 383
AM Access	Chapter 10, “RACF Access Monitor,” on page 643
EV Events	Chapter 7, “SMF and HTTP Reporting (Events menu),” on page 545
CO Commands	Chapter 17, “Setup and Library Commands,” on page 1641
IN Information	“IN INFORMATION - Information and documentation” on page 35
LO Local	“LO LOCAL - Locally defined options” on page 35

Primary commands

Primary commands can be entered at the command prompt (**===>**) on panels. Security zSecure supports the following primary commands.

ACCESS
The `ACCESS` command displays a panel to test the access of a third-party user or group to a resource. For more information, see the `CKGRACF ACCESS` command in Chapter 14, “CKGRACF Command Language,” on page 1499.

ACL
Use the ACL command to change the format and sort order of access lists (ACLs). You can enter this command on any display panel that has an access list. For RACF access lists, see “Access list display modes - reference material” on page 30.

C2RIMENU
This command is only meant to be used for problem determination. It can be used to display the results of the authority checks for the menu options to be shown and the actions to be shown on the menus. It is only enabled when the SETUP TRACE option `Debug action commands` is active. See “SE.T Setup - Trace” on page 1673 and “Debugging menu option and action character problems” on page 1580.

CARLA or COMM
Type CARLa commands.

CKXDEBUG
Display CKX diagnostic information. This command is only for problem determination. It is enabled only when the `SETUP TRACE` option *Collect CKX diagnostic* information is active. See “SE.T Setup - Trace” on page 1673.

CKNSERVE
Displays information about the zSecure Servers that are known to the zSecure Server address space identified by the ServerToken parameter on the CARLa OPTION command. See “ServerToken” on page 866.

COLS
Use the COLS command to show a ruler in the top of your screen. This ruler

simplifies determining the start or end column number where certain information can be found. These column numbers are frequently used on for example FIND commands. Use the command COLS OFF to remove the ruler when you no longer need it. The command abbreviation for `COLS` is `COL`.

FIELDS
Show all fields that can be used in CARLa queries, as described in "FIELDS - Show CARLa fields available" on page 35. The command abbreviation for FIELDS is FIELD.

FIND
Use the FIND command to perform a character string search for text in a display panel. The search includes all scrollable information in the report portion of the panel. The search excludes information in panel headers. The command abbreviation for FIND is F. To repeat the previous search, use RFIND command (PF5 key).

The FIND command supports parameters to define the following search characteristics: scan direction, starting point, column delimiters, and case-sensitivity.

Specifying the search argument
The character string text is the first argument of the FIND command. For example, to search for the string `ADGRANT`, at the panel command prompt, enter `FIND ADGRANT`.

In the search results, the cursor is positioned on the first character of the character string.

Strings that contain special characters, such as blanks, must be delimited with quotation marks (") or apostrophes(') for example: `'AD GRANT'`. Delimiters are required for special characters, but can be used on any search string.

Specifying parameters to indicate the start point and scan direction of the search

- **FIRST**

  Starts the search on the first line of the report and searches from top to bottom. The RFIND command (PF5) starts from the previous occurrence of the character and continues searching down.
- **LAST**

  Starts from the last line of the report and searches from bottom to top. The RFIND command (PF5) starts from the previous occurrence of the character string and continues searching up.
- **NEXT**

  Starts from the current cursor position and finds the next occurrence of the search argument. The search direction is top to bottom and left to right. The default setting is NEXT.
- **PREVIOUS**

  Starts from the current cursor position and finds the previous occurrence of the search argument. The search direction is bottom to top and right to left.

Specifying parameters to limit the screen columns included in the search

- **Use a column name**

  Limits the search to a single column. For example, to search for AD GRANT in the Name column only:

```
FIND 'AD GRANT' Name
```

- **Use one numerical limit**

  Limits the search to search arguments starting only on that character column. Note that the COLS primary command can be used to determine the character column position. For example, to search for AD GRANT only starting on character column 5:

  ```
  FIND 'AD GRANT' 5
  ```

- **Use a low and high numerical limit**

  Limits the search to search arguments occurring between two limits. Note that the COLS primary command can be used to determine the character column position. For example, to search for AD GRANT between character columns 10 and 25:

  ```
  FIND 'AD GRANT' 10 25
  ```

Specifying search parameters for case-sensitivity

The CAPS and ASIS parameters in combination with a literal-string search argument allow you to define case-sensitive and case-insensitive searches.

- **CAPS**

  The CAPS parameter is the default. If this parameter is used, or the ASIS parameter is not used, the search is case insensitive.

- **ASIS**

  The ASIS parameter is used for upper case searches and case-sensitive searches.

If the search argument is specified with quotes and prefixed by a C character to indicate a literal string, the search is case sensitive. For example to search for the string `Ad Grant`, enter:

```
FIND C'Ad Grant' ASIS
```

FORALL

Use the following procedure with the FORALL command to issue a command for all or selected profiles on a record-level display. The command abbreviation for FORALL is FOR.Use the following procedure with the FORALL command to issue a command for all or selected records on a record-level display. The command abbreviation for FORALL is FOR.

1. On a profile overview panel, the User Profile Overview panel (**RA.U**) panel for example, use the select (**Z** or **ZZ**) and exclude (**X** or **XX**) line commands to select the set of profiles you want to run the command on. See "Z - Select a profile" on page 74 and "X - Exclude profile line command" on page 74.

   If no selections are made, then all profiles are processed.

2. On command line, use one of the following methods to specify the command to be run:

   - Type the command directly behind the FORALL command as shown in the following example. Use the substitution variables described in Table 3 on page 14 to specify the command to run.

     ```
     FORALL LISTUSER !KEY  /* CLASS=!CLASS */
     ```

   - If the command is too long or if you want to reuse the command for other selections, type FORALL on the command line. Then, press **Enter** to open the FORALL Command Shell panel to specify the command.

     This panel is like the ISPF option 6 (TSO command shell) for entering commands that can be recalled for future use.

Depending on the SETUP CONFIRM options specified for your environment, the commands are either run immediately or queued in the CKRCMD file for viewing and editing before you submit them for processing.

Figure 5 shows a sample FORALL command to list the user profile for selected profiles on the User Profile Overview panel (**RA.U**).

```
zSecure Suite USER overview                              1 s elapsed, 0.5 s CPU
Command ===> FORALL LISTUSER !KEY  /* CLASS=!CLASS */_______   Scroll===> PAGE
Users like PYRL*                                  2 Sep 2010 20:59
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ PYRLAA1  SYS1     ANTONE ANDER         PYRL     PYRL     ____ ___          5
zz PYRLAA2  SYS1     ANTONE ANDER         PYRL     PYRL     ____ ___          5
__ PYRLAHI  SYS1     ANSEL HILLENBRA      PYRL     PYRL     RI   ___       X   1
zz PYRLAH2  SYS1     ANSEL HILLENBRA      PYRL     PYRL     RI   ___       X   1
__ PYRLBM2  SYS1     BILL MCMASTER        PYRL     PYRL     ____ ___          6
```

Figure 5. FORALL command for listing user profiles

In this example, the following command is run for all profiles in the selection block marked with the **ZZ** line command.

```
FORALL LISTUSER !KEY  /* CLASS=!CLASS */
```

The !KEY variable is replaced by the profile key of each of these users. This value is shown in the **User** column. The /* CLASS=!CLASS */ specification generates a comment that is appended to the LISTUSER command generated for each selected profile. For user profiles, !CLASS=*USER* for all profiles.

When this command is issued, it generates the following commands.

```
LISTUSER PYRLAA2 /* CLASS=USER */
LISTUSER PYRLAHI /* CLASS=USER */
LISTUSER PYRLAH2 /* CLASS=USER */
```

These commands are processed based on the SETUP CONFIRM options specified for your environment.

Table 3 shows the substitution variables available to specify the parameters for FORALL command processing. In the FORALL command, the following symbols have special meaning:

- Substitution variables are indicated by an exclamation point (!) immediately followed by a variable identifier that consists of letters, digits, national characters, hyphens, and underscores.
- A period (.) immediately following an identifier is interpreted as a separator, !KEY. for example.

If you want the actual exclamation point or period to be included in the command string, repeat the symbol, for example: !!. A double symbol is not interpreted as the beginning of a substitution variable or a separator. Other than scanning for exclamation points, the command is run in the same form specified in the FORALL parameter. It is not parsed in any way.

Table 3. FORALL command - Substitution Variables

Substitution Variable	**Meaning**
!CLASS	Represents the profile class. For example, on the User Profile Overview panel (**RA.U**) menu option, a FORALL command that includes !CLASS always replaces that variable with USER.
!GENERIC	Substitutes the word GENERIC for fully-qualified generic profiles only.

Table 3. FORALL command - Substitution Variables (continued)

Substitution Variable	Meaning
!KEY	Represents the profile key. For example, on the User Profile Overview panel (**RA.U**), the following command for user profiles issues a LISTUSER command for each profile. `"FORALL listuser !KEY"` For DATASET class profiles, quotes are added to comply with TSO command syntax. The !KEY for DATASET class profiles is the data set name. For MEMBER and R_AC1, the !KEY is the member name, and for DSN and SENSDSN, the !KEY is the data set name. For TRUSTED, the !KEY can be a RACF profile.
!KEY_MODIFIERS	Modifiers to disambiguate the profile key. For example, on the Data set overview panel (**RA.D** menu option), the following command issues the LISTDSD command for each profile. `FORALL listdsd da(!key) !key_modifiers` The !key_modifiers parameter provides the GENERIC keyword where needed for fully-qualified generic profile as well as the VOL(...) clause for discrete profiles.
!TYPE	Indicates the profile type, GENERIC or NONVSAM for example.
!VOLSER	The volume serial disambiguates the key of a discrete profile. This substitution variable does not include the VOL(and) parts that are present in !KEY_MODIFIERS.

HELP

The HELP command is equivalent to the PF1 key. You can ask for help at any time. Most important screens have context-sensitive help. Other screens present the application tutorial. To get help on a field, position the cursor on the field or column and press PF1. To get help on a panel, position the cursor on the command line in the ISPF panel. Then, press PF1.

MESSAGE, MSG, or MSGS

Show the message library, or look up a message. The explanatory text displayed is documented in the *IBM Security zSecure: Messages Guide*.

Example:

The following command looks up message CKR0010 in the Security zSecure message library.

```
MSG 10
```

The following command looks up message CKF039I in the zSecure Collect message library.

```
MSG CKF039I
```

The following command looks up message CKG100I in the zSecure Collect message library.

```
MSG CKG100I
```

MODIFY

Use the MODIFY command to enable or disable the ability to change values of modifiable fields. The MODIFY command accepts the parameters ON or OFF. The

command abbreviation for MODIFY is M. If `MODIFY` is entered without a parameter, it reverses the current `MODIFY` setting.

PRT, PRTLIST
Create a hardcopy of a display, written to the standard ISPF LIST data set. This command is available only on display panels. You can print the LIST data set from any ISPF panel by issuing the `LIST` primary command. The ISPF LIST command can also be issued from outside Security zSecure.

RACF
Use the `RACF` command from zSecure display panels to open the RACF ISPF panels. When you are done working in the RACF ISPF panels, enter the `END` command or press `PF3` to return to the zSecure display panel.

RESET
Use the `RESET` command to remove all pending updates from display panels and cancel pending commands. One common use of this command is to remove an incorrect entry in a modifiable field and reset the incorrect entry to the original (valid) entry. The command abbreviation for RESET is RES.

RESULTS
Use the `RESULTS` command from menu and selection panels to open the Results panel. On the Results panel, you can choose to view results from the last query, any commands generated, the message output, and so on. The command abbreviation for RESULTS is RESULT. For more information, see "RESULTS - View output and results" on page 24.

RFIND
Repeat the previous FIND command from the current cursor position. This command is available only on display panels. Usually, you can also use F5 key to run the RFIND command.

SET
Use the `SET` command as an alternative way to change some options on the Setup - View and Setup - Confirm display panels. When you issue the SET command on a display panel, the changed options are applied immediately. For more information, see "SE.5 Setup - View" on page 1659 and "SE.4 Setup - Confirm" on page 1655.

SETUP
Invoke the SETUP application, as described in Section "SE SETUP - Options and input data sets used" on page 1641. Specify a number from the SETUP option menu to go directly to that option, SETUP 1 for example to select a different input source. The options are also available by name. For example, type SETUP FILES to select a different input source.

SORT
Use the `SORT` command on record-level display panels to sort results. The command abbreviation for SORT is SO. By default, result lines are sorted alphabetically in ascending order starting with the left column, in this example: **Userid**, then **Name**, **More data**, and **Even more data**.

Userid	Name	More data	Even more data
KEY1	MY_NAME	OTHER_VALUE	BREAD
KEY2	HIS_NAME	MORE_VALUES	HALIBUT
KEY3	HIS_NAME	NEW_VALUE	SODA

To sort result lines using any other column, enter the column name followed by the sort order: `A` or `ASCENDING`, or `D` or `DESCENDING`. For example, `SORT "Name" Ascending` produces the following results:

Userid	Name	More data	Even more data
KEY2	HIS_NAME	MORE_VALUES	HALIBUT
KEY3	HIS_NAME	NEW_VALUE	SODA
KEY1	MY_NAME	OTHER_VALUE	BREAD

To sort result lines using multiple columns, for example, `SORT "Name" A "More data" D` produces the following results:

Userid	Name	More data	Even more data
KEY3	HIS_NAME	NEW_VALUE	SODA
KEY2	HIS_NAME	MORE_VALUES	HALIBUT
KEY1	MY_NAME	OTHER_VALUE	BREAD

The `SORT` command cannot be used on detail display panels; instead, use the `ACL SORT` command. The `SORT` command cannot be used on static ISPF section panels.

STARTPAN
Specify the panel that opens when zSecure starts. See Section "Start Panel - Setting your favorite menu as the entry panel" on page 1641 for more information about start panels.

SYSPREV
Use the `SYSPREV` command to browse the `SYSPRINT` message file of a recursive query. You can enter the `SYSPREV` command from any display panel if the last task used a recursive query.

SYSPRINT
Use the `SYSPRINT` command to browse the message output file of the report generated from the last query. Exit the generated report by using `PF3` or `END`. Issue the `SYSPRINT` command from a menu or selection panel. An error displays if you enter `SYSPRINT` from the panel on which the generated report is displayed.

TEMPLATE
Show the contents of the RACF database templates, as described in Section "TEMPLATE - Template field properties" on page 284.

A sample run

As a first introduction to Security zSecure, this section presents a sample run. You can try running this sample on your system to see what happens. In this example, you learn how to view the user profiles and change them. You also learn how to use the commands generated by Security zSecure.

For additional information about a panel, press the `PF1` key to access the online help. To get information about a particular field or column, place the cursor on the field or column, then press `PF1`.

First, set the Security zSecure *options* for this example, in order to prevent any unwanted changes to the RACF database. Type **SETUP CONFIRM** or go to **SE.4** and enter all options as displayed in the following figure. The meaning of these options is explained later. When you exit the Security zSecure program, these options are automatically saved for the next session.

```
  Menu         Options       Info    Commands     Setup
_______________________________________________________________________________
                          zSecure Suite - Setup - Confirm
Command ===> _____________________________________________________________________

Action on command . . 1  1. Queue    2. Execute  3. Not allowed
Confirmation  . . . . 4  1. None     2. Deletes  3. Passwords      4. All
Command Routing . . . 3  1. Ask      2. Normal   3. Local only

Command generation
Enter "/" to select option(s)
/  Overtype fields in panels
/  Change generated commands
/  Specify start/end date
/  Generate SETROPTS REFRESH commands
   /  Issue prompt before generating SETROPTS REFRESH commands
Commands to generate
/  RACF commands
/  CKGRACF commands
/  CKGRACF ASK for later execution
/  CKGRACF REQUEST for later execution
_  CKGRACF WITHDRAW queued commands
/  CKGRACF RDELETE commands
```

Figure 6. Setup Confirm Menu

Press **End** when you are done to return to the main menu.

Select the RACF ADMIN selection menu by typing **RA** on the command line of the main menu; then press ENTER. You see the RACF ADMIN selection menu; these menus are used to select and display RACF profiles. Now type **U**. You see the USER SELECTION panel, displayed in Figure 7.

```
  Menu   Options   Info   Commands   Setup
-------------------------------------------------------------------------------
                          zSecure Suite - RACF - User Selection
Command ===> _____________________________________________     start panel

_   Add new user or segment

Show userids that fit all of the following criteria
Userid  . . . . . . *________    (user profile key or filter)
Name  . . . . . . . _____________________________ (name/part of name, no filter)
Installation data . _____________________________ (data scan, no filter except *)
Owned by  . . . . . _________    (group or userid, or filter)
Default group . . . _________    (group or filter)
Connect group . . . _________    (group or filter)

Additional selection criteria
_  Other fields       _  Attributes       _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Specify scope
_  Print format       _  Customize title  _  Send as e-mail
   _  Background run  _  Full page form   _  Sort differently  _ Narrow print
```

Figure 7. Display User Menu

This is the basic selection panel, additional selection panels are shown when you select (/) any of the fields under "Additional selection criteria". The additional selection criteria are used only when you select the fields, but the selections are remembered as long as you are using the RA.U option.

The User Selection panel selects user IDs that match your search criteria. For now, do not specify anything. Press ENTER. IBM Security zSecure prompts for confirmation that you want to scan the whole database by putting an asterisk in

the **Userid** field and displaying the message `Default prompting`. By pressing ENTER a second time, the query starts, and presents a display with the results. A sample display is shown in Figure 8.

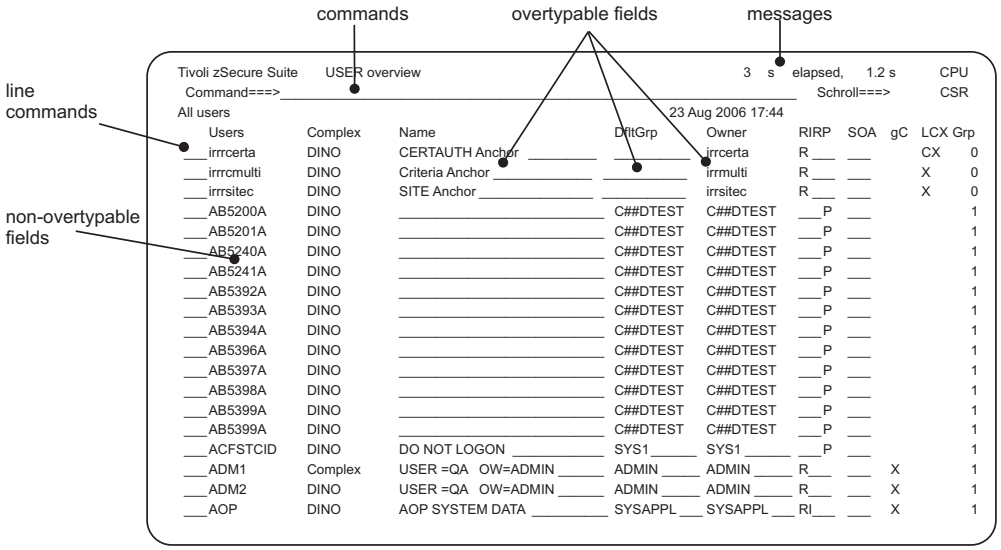


Figure 8. Overview Display

This display is an *overview* or *record* display, in which each profile is displayed on a single line. Scroll up and down, or left and right, to view more information. (A *detail* display showing one profile in detail also exists; more about this later.)

In the line command position in front of each user ID, you can issue a one- or two-character command. On the overview panel, a line command works on the entire profile. Several line commands are available for use depending on your authorization level, the installed and active Security zSecure product components, and the profile type. To see the available line commands in a popup window, type a slash (/) in front of the userid.

Also note the fields indicated as *modifiable fields*, for example the **Name** field. Modifiable fields are highlighted or shown in a different color depending on your CUA settings. You can change the settings with the ISPF primary command **CUAATTR**. If you type a new value over a modifiable field and press **Enter**, Security zSecure generates a command to change the profile to the new value.

To show command generation, change a user name (**Name**). Then, press **Enter**. A command confirmation panel is displayed to accept or cancel the command. For example, Figure 9 on page 20 shows the configuration panel that shows if the name for `userid` *ADGRANT* is changed to *ARTHUR GRANT*.

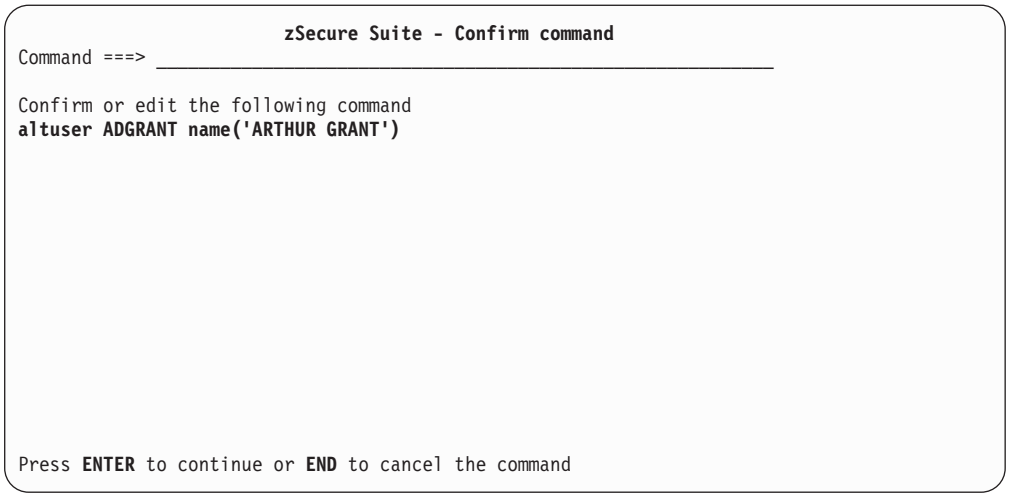


Figure 9. Confirmation Panel

Press **Enter** to accept the command. The command is not run because we specified the Queue option in SETUP CONFIRM panel. On any confirmation panel, you can cancel the command by pressing **End**, or accept it by pressing **ENTER**. You can change the circumstances in which confirmation is requested on the SETUP CONFIRM panel. ALL, the current setting is the safest option. See also "SE.4 Setup - Confirm" on page 1655.

After pressing **Enter**, the top right of the screen reads Queued in CKRCMD. This message indicates that the command you just confirmed was not run. Instead, it was stored in the CKRCMD command output file for later execution. The use of the CKRCMD file instead of direct execution of the command is another safe option set on the SETUP CONFIRM panel. If you set the **Action** parameter to EXECUTE, the command is executed immediately and not queued. The EXECUTE option is often more practical than QUEUE, but when you are learning to use Security zSecure, it is safer to queue commands rather than run them immediately.

To copy the profile, type **C** in the entry field for a profile. The USER COPY panel shown in Figure 10 on page 21 opens so you can specify a new user ID for the copy.

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - User copy
Command ===> ____________________________________________________________

From userid . . . . . : ADGRANT
To id . . . . . ________  Name  . . . . . QQLQ
Password  . . . . . ________
Password phrase . . . . ____________________________________________________
_____________________________________ (9-100 chars, in single quotes)
Name  . . . . . ARTHUR GRANT
Owner . . . . . SYSUSER  Default group . . . . . SYSUSER
Installation data . . . ____________________________________________________
________________________________________________________________________________
________________________________________________________________________________
_____________________________________
_  Copy permits only (target id may be a group or a user)
_  Generate RACF commands when the target user exists
_  Copy USERDATA and CUSTOMDATA
_  Specify unique segment data
_  Revoke new userid             _  Protected
_  Copy catalog aliases (only if CKFREEZE is present)
/  Issue ADDSD/RDEF for dataset and resource profiles related to the user
/  Copy RACFVARS profiles/members too
```

Figure 10. USER COPY Panel

On this panel, specify a new `userid` and password, and press ENTER. This results in the generation of the necessary RACF commands for creating the new user. These commands are added to the `CKRCMD` file. Figure 7 on page 18 is shown, with the message `Commands queued, RC=`*`rc`*. If you press END, you see the generated commands. If you press END again, you see the RESULTS panel. Press the END key again to return to the selection screen.

You are now back at the user selection screen, press ENTER to display all users again.

Now put the cursor in front of a profile (at the first column of the line command field) and press ENTER. This is equivalent to typing S in front of the profile. A *detail display* is shown with information about the single user profile you selected on the overview display. You can return to the overview display by pressing the END key. A sample detail display is shown in Figure 11 on page 22.

```
zSecure Suite USER overview                                  Line 1 of 39
Command ===>                                                 Scroll===> CSR
All users                                    26 Nov 1998 07:47


_ Identification of ADGRANT                                          IPO1
  User name                    AD GRANT_____________
  Installation data            ____________________________________________
_ Owner                        SYSUSER_
_ User's default group         SYSUSER_

  Group    Auth    R SOA AG Uacc    Revokedt    Resumedt    InstData
_ SYSUSER_ USE____ _ ___ __ READ___ ___________ ___________
_ SYS1____ USE____ _ ___ __ READ___ ___________ ___________
_ ADMGRP__ JOIN___ _ Y__ __ READ___ ___________ ___________

  System access                          Statistics
  Revoked (may be by date)      No_      Creation date                 18Jul96
  Inactive, revoked or pending  No       Last RACINIT current connects 20Jul00
  Days of week user can logon   SMTWTFS  User's last use date          20Jul00
  Time of day user can logon    _________ User's last use time         18:51
  Date user will be revoked     ___________ (ddmmmyyyy or NOREVOKE)
  Date user will be resumed     ___________ (ddmmmyyyy or NORESUME)

  Password                               Password phrase
  Has a password                Yes      Has a password phrase         Yes
  Expired password              No       Expired password phrase       No
  Password changed date         23Mar06  Password phrase change date   23Mar06
  Password expiration date      21Aug06  Password phrase expiry date   21Aug06
  Old passwords present #         1      Old pass phrases present #    2
  Failed password attempts #      0
  Password interval             _90
  Password interval in effect    90
  Mixed case password           Yes
  Has a password envelope
  Password disabled   PROTECTED No_

  Mandatory Access Control               Privileges
  Security label                ________ Security admin        SPECIAL No_
  Security level                         DASD administrator OPERATIONS No_
  Categories list                        Global audit set/list AUDITOR No_
  Class authority               ________

  Safeguards
  Ignore UACC/Glob/* RESTRICTED No_
  Log all user actions   UAUDIT No_
  Digital certificate labels      Digital certificate names
  ________________________________
  Certificate filter label
  ________________________________

  Identity mapping label   Identity mapping filter                      Identi
_ myFirstRACMAP            UID=armeBert,OU=Tools Development,O=IBM,C=NL  ldaps.c
****************************** BOTTOM OF DATA *******************************
```

Figure 11. Detail Display

The detail display (which is a scrollable panel) also supports line commands and modifiable fields. On this panel, the line commands apply to fields within the profile, not the profile itself.

On this panel, you can experiment with modifiable fields and line commands. As long as you leave the CONFIRM settings so that you can cancel any changes, you cannot do any harm to your security database. If you type an illegal value on a field, the field is highlighted (usually in red); in this case, the RESET command can be used to reset the field to its previous value. When you are done, press END on the overview display (Figure 8 on page 19), or END twice from a detail display (Figure 11). Now, let's go and see what became of the commands written to CKRCMD.

The display in Figure 12 shows the CKRCMD file. This file is shown in an editor so you can modify, add, or delete the commands as required.

```
EDIT      GRPADM1.C2R1EF2A.CKRCMD                       Columns 00001 00072
Command ===>                                               Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001         /* CKRCMD file CKR1CMD complex DINO generated  2 Feb 1999 12:36
000002         altuser ADGRANT name('ARTHUR GRANT')
000003         /* CKRCMD file CKR1CMD complex DINO generated  2 Feb 1999 12:37
000004          /* Commands generated by COPY USER/GROUP  */
000005         adduser ADGRANT1  password(SDGFDGSG) +
000006             name('AD GRANT   ') +
000007             owner(SYSUSER) +
000008             dfltgrp(SYSUSER)
000009          altuser ADGRANT1 revoke
000010          password user(ADGRANT1) interval(30)
000011          connect ADGRANT1 group(SYSUSER) owner(SYSUSER)  auth(USE) uacc(
000012          connect ADGRANT1 group(SYS1) owner(SYS1)  auth(USE) uacc(READ)
000013          connect ADGRANT1 group(ADMGRP) owner(ADMGRP)  auth(JOIN) uacc(R
****** *************************** Bottom of Data ***************************
```

Figure 12. CKRCMD Output File

Delete all commands in the CKRCMD file, then add a single LISTUSER command for your userid. Start commands in column nine. Leave the first eight columns because these are ignored when executing the command file (reserved for line numbers). Figure 13 shows an example of the CKRCMD file.

```
EDIT      GRPADM1.C2R1EF2A.CKRCMD                       Columns 00001 00072
Command ===>                                               Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001         listuser GRPADM1
****** *************************** Bottom of Data ***************************
```

Figure 13. Edited CKRCMD Output File

Make sure that the LISTUSER command is the only command left in the CKRCMD file, then press END.

You then see the RESULTS display which contains all the results from the Security zSecure run. The cursor is positioned in front of the CKRCMD line.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Results  Enter R to run commands
Command ===> ____________________________________________________________

The following selections are supported:
 B Browse file               S Default action (for each file)
 E Edit file                 R Run commands
 P Print file                J Submit Job to execute commands
 V View file                 W Write file into seq. or partitioned dataset
 M E-mail report

Enter a selection in front of a highlighted line below:
 _ SYSPRINT  messages
 _ REPORT    printable reports
 _ CKRTSPRT  output from the last TSO command(s)
 _ CKRCMD    queued TSO commands
 _ CKR2PASS  queued commands for Security zSecure
 _ COMMANDS  Security zSecure input commands from last query
 _ SPFLIST   printable output from PRT primary command
 _ OPTIONS   set print options

 _ View files from recursive call (now on level 0)
```

Figure 14. Results Display

On the RESULTS display, any selectable option is highlighted. To run a command for one of the listed files, enter the command abbreviation in the entry field for the file. For example, to edit the CKRCMD file, type an **E** in the entry field for the CKRCMD file again. Then, press **Enter**.

You can also run a command saved in the CKRCMD file. Make sure that the CKRCMD file contains only the harmless LISTUSER command, type an **R** in the entry field for the CKRCMD file and press **Enter**. The LISTUSER command is run, and the result (a description of your `userid`) is displayed on the terminal.

If you press **END** on the Results panel, you return to the Security zSecure User Selection panel (Figure 7 on page 18). To reopen the Results panel, type `RESULTS` on the command line at the top of the screen.

This example shows the basic operation of Security zSecure. If you leave the `CONFIRM` option to a safe setting, and do not execute the commands generated, you can safely explore the other menu options. For more detailed examples and explanations, see the *IBM Security zSecure Admin and Audit for RACF: Getting Started Guide*.

To use the ISPF online help, place your cursor on the command line and press `PF1` to open the help panel for that panel. If you press `PF1` with the cursor in a field, a help panel opens with a description of the current field.

RESULTS - View output and results

The Results panel is displayed after a run if any of the files CKREPORT, CKRCMD, or CKR2PASS contains program output. It can be called up at any time using the `RESULTS` primary command.

The options that can be used are highlighted on the menu. For example, to browse the TSO commands, type a **B** in front of CKRCMD. If the program generated second-pass commands, these are stored in CKR2PASS. Type **R** in the input field in front of the CKR2PASS entry to run the commands.

Use this panel to edit, browse, or run the indicated files.

```
   Menu   Options   Info   Commands   Setup
 ------------------------------------------------------------------------------

                          zSecure - Results  Enter R to run commands
Command ===> ____________________________________________________________

The following selections are supported:
  B Browse file               S Default action (for each file)
  E Edit file                 R Run commands
  P Print file                J Submit Job to execute commands
  V View file                 W Write file into seq. or partitioned dataset
  M E-mail report

Enter a selection in front of a highlighted line below:
_ SYSPRINT  messages
_ REPORT    printable reports
_ CKRTSPRT  output from the last TSO command(s)
_ CKRCMD    queued TSO commands
_ CKR2PASS  queued commands for Security zSecure
_ COMMANDS  Security zSecure input commands from last query
_ SPFLIST   printable output from PRT primary command
_ OPTIONS   set print options
```

Figure 15. Results Display - Available options

Valid selections are described in the following table.

Table 4. Results Display - commands available

Command	Action
B	Browse the file
E	Edit the file
G	Same as R
J	Submit a batch job to run the commands in the file
M	Email the file
P	Print the file, using the print options determined by the OPTIONS menu
R	Run the commands in the file
S	Default action. The default is different for each file.
V	View the file
W	Write the file into a (sequential or partitioned) data set

SYSPRINT
This file contains messages describing the results, and any errors, from the last program run. Messages generated by `VERIFY` commands, and output from the `SHOW` command is also written to this file. Valid selections for this file are `S`, `B`, `E`, `P`, `V`, `M`, and `W`. The default action is browse.

REPORT
This file contains output from queries in Print Format. Valid selections for this file are `S`, `B`, `E`, `P`, `V`, `M`, and `W`. The default action is browse.

CKRTSPRT
This file contains output from the last TSO commands. Valid selections for this file are `S`, `B`, `E`, `P`, `V`, `M`, and `W`. The default action is browse.

CKRCMD
If the command action is set to `QUEUE`, this file contains `TSO` commands

generated by , VERIFY, COPY, MOVE, and REMOVE commands, as well as commands generated by line commands or modified fields. This can include RACF, CKGRACF, and IDCAMS commands. This release does not yet support generating ACF2 commands. Valid selections for this file are S, B, E, P, V, M, W, R, or G. The default action is edit.

All commands generated in one run are **added** only to the CKRCMD file. The file is emptied only when a new initial query is performed.

You can edit and run only the commands from the lowest level of the query **not** from recursive calls to Security zSecure. An error message is generated if you try to run or edit the file from the wrong level.

If you selected multiple complexes, multiple CKRCMD files are used. When you select the CKRCMD file, an extra selection panel opens like the one shown in Figure 16.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - Results  Use END for other files
COMMAND ===>                                                 Scroll ===> CSR

The following selections are supported:
 B Browse file               S Default action (for each file)
 E Edit file                 R Run commands
 P Print file                J Submit Job to execute commands
 V View file                 W Write file into seq. or partitioned dataset
 M E-mail report

CKRCMD for the specified environments:

     Complex  Njenode   Rrsfnode   System     zSecNode #Lines
   _ DINO     JES2DINO  DINO       DINO       ?        2
   _ CNRLPROG C##4      C##4       C##4       ?        1
****************************** Bottom of data ********************************
```

Figure 16. Results Display - CKRCMD file

All actions specified are performed only on the selected CKRCMD.

CKR2PASS
This file contains IBM Security zSecure commands generated by line commands on profiles. These commands are always queued, and can be executed by typing **R** or **J** in the selection field for **CKR2PASS**. Valid selections for this file are S, B, E, P, V, M, W, R, or G. The default action is edit.

COMMANDS
This file contains the input commands from the last run of the program. Valid selections for this file are E, S, M, and /. Use the E, S, and / actions to edit the commands. You can change, run, or submit the commands or save them to a private data set.

SPFLIST
The ISPF LIST data set contains printable output generated by the program when the PRT command was issued on a display. Valid selections for this file are M, S and /. The S and / actions lead to the ISPF List panel.

OPTIONS
Set print options. Valid selections for this file are S and /. Both actions lead to the Print Options panel.

Recursive calls

From a record display, it is often possible to invoke another, more detailed record display. This action is known as a recursive call. Any commands queued by recursive calls are saved in the same CKRCMD file. These commands can be executed when you leave the initial display. You can view the SYSPRINT output from a recursive call by issuing the SYSPREV primary command or through the Results panel by selecting one of the files listed at the bottom of the panel.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - Results
Command ===> ____________________________________________________________

The following selections are supported:
 B Browse file                S Default action (for each file)
 E Edit file                  R Run commands
 P Print file                 J Submit Job to execute commands
 V View file                  W Write file into seq. or partitioned dataset
 M E-mail report

Enter a selection in front of a highlighted line below:
_  SYSPRINT  messages
_  REPORT    printable reports
_  CKRTSPRT  output from the last TSO  command(s)
_  CKRCMD    queued TSO commands
_  CKR2PASS  queued commands for Security zSecure
_  COMMANDS  Security zSecure input commands from last query
_  SPFLIST   printable output from PRT primary command
_  OPTIONS   set print options

_   View files from recursive call (now on level 0)
```

Figure 17. Results Display - Recursive calls

CKRCMD - Viewing and executing commands

When selecting a CKRCMD file you are presented with the standard ISPF editor, with the file loaded.

```
File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       C##BDV2.C2R1EF2A.CKRCMD                       Columns 00001 00072
Command ===>                                                 Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001         /* CKRCMD file CKR1CMD complex DINO NJE JES2DINO generated 10 No
000002         listuser C##BDV2
000003         rdelete APPCTP   DBTOKEN1.LEVEL.JOE.MAIL.PGM.LONGQUALIFIER$AND$A
000004         rdelete SURROGAT MYUSER.SUBMIT
000005         altdsd 'C##QARUN.NOOWNER.**' generic owner(C##QARUN)
000006         SETROPTS REFRESH RACLIST(SURROGAT) /* POSIT 104 */
000007         SETROPTS REFRESH GENERIC(DATASET)
****** **************************** Bottom of Data ****************************
```

Figure 18. CKRCMD file - editing

After verifying the commands generated and editing them where necessary, press **END**. Then, enter the **R** (Run) line command to run the commands.

If Command Routing is set to Ask you will be asked to select command destinations before the command is executed. For more information see "Command routing" on page 28.

A Results panel like the one shown in Figure 19 opens for reviewing the outcome of the command operations.

```
BROWSE    C##BDV2.C2R1EF2A.CKRTSPRT                  Line 00000000 Col 001 080
Command ===>                                                  Scroll ===> CSR
******************************** Top of Data ********************************
================================================================================
=== Multiple TSO command output file - scroll max down for overview ===
=== Input dataset C##BDV2.C2R1EF2A.CKRCMD                                  ===
================================================================================
/* CKRCMD file CKR1CMD complex DINO NJE JES2DINO generated 10 Nov 1999 15:14 */

============ 10Nov1999  16:30:23.88 start record 2 ============
listuser C##BDV2
USER=C##BDV2  NAME=DANIELLE VUKOVICH     OWNER=C##B      CREATED=98.358
 DEFAULT-GROUP=C##B      PASSDATE=99.263  PASS-INTERVAL= 90
 ATTRIBUTES=NONE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=99.314/10:27:19
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ---------------------------------------------
 ANYDAY                          ANYTIME
  GROUP=C##B      AUTH=USE      CONNECT-OWNER=C##B      CONNECT-DATE=98.358
    CONNECTS=   545  UACC=NONE     LAST-CONNECT=99.314/10:27:19
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
============ 10Nov1999  16:30:23.93 start record 3 ============
rdelete APPCTP   DBTOKEN1.LEVEL.JOE.MAIL.PGM.LONGQUALIFIER$AND$A$KEY$WITH$A$LENG
ICH12103I NOT AUTHORIZED TO DELETE DBTOKEN1.LEVEL.JOE.MAIL.PGM.LONGQUALIFIER$AND
CKX962F Command failed, return code 4 (decimal)

============ 10Nov1999  16:30:23.99 start record 4 ============
rdelete SURROGAT MYUSER.SUBMIT
ICH12103I NOT AUTHORIZED TO DELETE MYUSER.SUBMIT.
CKX962F Command failed, return code 4 (decimal)

============ 10Nov1999  16:30:24.04 start record 5 ============
altdsd 'C##QARUN.NOOWNER.**' generic owner(C##QARUN)
ICH22005I NOT AUTHORIZED TO ALTER C##QARUN.NOOWNER.**
CKX962F Command failed, return code 4 (decimal)

============ 10Nov1999  16:30:24.24 start record 9 ============
SETROPTS REFRESH RACLIST(SURROGAT) /* POSIT 104 */
ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS.
CKX962F Command failed, return code 8 (decimal)

============ 10Nov1999  16:30:24.28 start record 10 ============
SETROPTS REFRESH GENERIC(DATASET)
ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS.
CKX962F Command failed, return code 8 (decimal)
================================================================================
=== Failed command start record numbers                                    ===
===  3 4 5 6 7
================================================================================
****************************** Bottom of Data ******************************
```

Figure 19. CKRTSPRT - results of command execution

Command routing

If you set Command Routing to **Ask** on the panel "SE.4 Setup - Confirm" on page 1655, the following panel is displayed before a command is executed.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                      zSecure Admin+Audit for RACF - Command   Line 1 of 11
Command ===>                                              Scroll ===> CSR
Normal destination is *LOCAL*
Enter L/A/O/Z/J to select one or more nodes to execute the commands.
S L Sysname  SID  RRSFNode zSecNode NJENode  Userid   A  O      Z    J
                           DINOPLEX                             ZSEC
    EZOS     EZOS EZOS     EZOSPLEX JES2EZOS C##BUR1  AT ONLYAT ZSEC NJE
    EZOS     EZOS EZOS     EZOSFRGN JES2EZOS C##BUR1  AT ONLYAT ZSEC NJE
    E1A0     E1A0 E1A0     E1A0PLEX JES2E1A0 C##BUR1  AT ONLYAT ZSEC NJE
  * NMPIPL87 IPO1 NMPIPL87 NMPIPL87 NMS87    C##BUR1  AT ONLYAT ZSEC NJE
    OTHRSYS8      MAINOTHR                   C##BUR1  AT ONLYAT
                  DINO                       C##BUR1  AT ONLYAT
```

Figure 20. RACF command routing panel

Figure 20 displays the available command routing destinations or nodes. There are three types of nodes:

RRSF
Nodes are defined by RACF. RACF commands only are directed via the AT or ONLYAT parameter.

ZSEC
Nodes are defined by zSecure Server. The local zSecure server will transmit the commands to the remote system. On the remote system, commands are executed by the remote zSecure server.

NJE
Nodes are defined by JES2. The commands are executed using a batch job which is routed to the remote system.

Each row in Figure 20 represents a single system unless multiple nodes of the same type exist for a single system. The system name and system ID are displayed in columns **Sysname** and **SID**. The RRSF, ZSEC and NJE node names are displayed in the **RRSFNode**, **zSecNode**, and **NJENode** columns.

One node can be chosen from each row using the L, A, O, Z or J selection characters.

Selection character	Description
L	Route command to the local system.
A	Route command to the RRSFNode using the RRSF AT() parameter.
O	Route command to the RRSFNode using the RRSF ONLAT() parameter.
Z	Route command to the zSecNode.
J	Route command to the NJENode.

RRSF routing is implemented by appending the AT() or ONLYAT() parameters to the command. Only RACF commands will be able to be routed using RRSF. The command is issued locally and RACF performs the routing. The **Userid** column indicates the userid that is used for the RRSF AT() and ONLYAT() parameters.

The **A**, **O**, **Z**, and **J** columns in the preceding table indicate what particular routing method is available.

The **L** column displays a character to indicate when a row is considered to be the local or normal node.

=	This is the local node. The command is directed here if you select **Local only** for the Command Routing selection on the "SE.4 Setup - Confirm" on page 1655 panel.
>	This is the normal node. The command is directed here if you select **Normal** for the Command Routing selection on the "SE.4 Setup - Confirm" on page 1655 panel.
*	This node is both local and normal.

Access list display modes - reference material

This section describes more advanced zSecure options that you might want to skip until you have mastered basic operation of IBM Security zSecure.

When RACF shows an access list, it only shows the RACF IDs and access levels. Finding out the access each user has can be difficult if the user is connected to many groups. Security zSecure can display the access list in the following ways so you can investigate each user access: *exploded*, *resolved*, *effective*, and *trust*. In addition, you can further customize the access lists using the `SCOPE` and `NOSCOPE` and the `UNIVERSAL` and `NOUNIVERSAL` commands.

The display mode can be changed interactively with the `ACL` command or specified as an output modifier.

An *exploded* access list shows every way in which a user has access to a profile. All group access list entries are expanded by entries for each user in the group. If a user is connected to multiple groups on the access list, the `userid` is shown multiple times. Access due to a group-operations or operations attribute is shown as well. In addition, administrative access through group-special or ownership is shown as `OWNER` and administrative access through a High-level qualifier is displayed as `QUALOWN`. You can remove this access information from the view by issuing a `NOSCOPE`. You can also sort the access list to view access by level, group, or userid. An exploded access list is especially helpful if you want to remove a user or group from an access list and you are unsure how many ways that access is granted.

A *resolved* access list shows the actual access that a user has to a profile. If a user is on the access list, that entry is displayed. If a user is not on the access list but some of the connect groups for the user are on the access list, the *highest* access that the user has through any of the connect groups is displayed. Administrative authority can be taken into account by using the *scope* toggle. In that case, administrative access is considered higher than normal access through the access list.

An *effective* access lists shows the effective access that a user has to a profile. The effective access list is the resolved access list extended with entries for users that are not explicitly on the access list but have access due to a group operations or operations attribute, these show the access level ALTER-O and the group concerned, or `- oper -`, respectively. Administrative authority can be taken into account by using the *scope* toggle. In that case, administrative access is considered higher than normal access through the access list.

A *trust* access list shows the actual access that a user has to a profile, as well as the administrative access. It shows all ways in which the user currently has data access. In addition to this data access, administrative authority through group-special or ownership is displayed as OWNER and administrative access through a High-level qualifier is displayed as QUALOWN. The trust access list shows exactly the trust relations that are considered for the TRUSTED report types if the profile protects a sensitive resource.

The effect of the SCOPE and NOSCOPE toggle is visible for all except normal access lists. SCOPE shows administrative access through group-special or ownership as OWNER and administrative access through a High-level qualifier as QUALOWN, NOSCOPE eliminates the administrative access. The default effect is NOSCOPE for output modifiers EXPLODE, RESOLVE, and EFFECTIVE, as well as for ISPF ACL commands ACL NORMAL, ACL RESOLVE, and ACL EFFECTIVE. The default is SCOPE for the ISPF ACL commands ACL EXPLODE and ACL TRUST.

The effect of the UNIVERSAL and NOUNIVERSAL toggle is the same for all types of access list. If UNIVERSAL is specified default connections to universal groups–that is, connections with USE authority and no group special, operations, or auditor attributes–are taken into account, as well as the access granted by system-wide operations, if applicable to the type of access list shown. If NOUNIVERSAL is specified neither default connects to universal groups nor system-wide operations users are included in the access list.

The following tables show examples of exploded and resolved access lists. It uses five users (USER1, USER2, USER3, USER4, and USER5) and two groups. GROUP12 consists of USER1 and USER2. GROUP234 consists of USER2, USER3, and USER4. The following table shows the actual access list. All the following examples assume that the UNIVERSAL and NOUNIVERSAL toggle is set to UNIVERSAL.

The normal access list as displayed after an ACL NORMAL command which sets the scope attribute to NOSCOPE.

Table 5. Normal Access List

User	Access	Access List id
USER1	READ	USER1
USER2	UPDATE	USER2
USER3	NONE	USER3
-group-	CONTROL	GROUP12
-group-	READ	GROUP234

The following table shows the exploded access list as it would be after an ACL EXPLODE command. An ACL EXPLODE command turns on SCOPE automatically. It shows every way the user might have access. Note that the groups are no longer included in the leftmost column.

Table 6. Exploded Access List (EXPLODE, SCOPE modifiers or ACL EXPLODE)

User	Access	Access List id
USER1	OWNER	USER1
USER1	CONTROL	GROUP12
USER1	READ	USER1
USER2	CONTROL	GROUP12

Table 6. Exploded Access List (EXPLODE, SCOPE modifiers or ACL EXPLODE) (continued)

User	Access	Access List id
USER2	UPDATE	USER2
USER2	READ	GROUP234
USER3	READ	GROUP234
USER3	NONE	USER3
USER4	READ	GROUP234
USER4	ALTER-O	- oper -
USER5	ALTER-O	- oper -

The Resolved Access List table shows the actual way the user has access when using the `RESOLVE` modifier or the ISPF command `ACL RESOLVE`. A user ID on the access list overrides any group access. If several group accesses are included, the highest is used.

Table 7. Resolved Access List (RESOLVE modifier or ACL RESOLVE)

User	Access	Access List id
USER1	READ	USER1
USER2	UPDATE	USER2
USER3	NONE	USER3
USER4	READ	GROUP234

The Effective Access List table is like the Resolved access list with the exception that system-wide operations and group-operations are taken into account.

Table 8. Effective Access List (EFFECTIVE modifier or ACL EFFECTIVE)

User	Access	Access List id
USER1	READ	USER1
USER2	UPDATE	USER2
USER3	NONE	USER3
USER4	READ	GROUP234
USER5	ALTER-O	- oper -

Table 9 shows the resolved access list with scope activated, as it would be when changing from explode to resolve):

Table 9. Resolved Access List with scope (RESOLVE, SCOPE modifiers or ACL RESOLVE SCOPE)

User	Access	Access List id
USER1	OWNER	USER1
USER2	UPDATE	USER2
USER3	NONE	USER3
USER4	READ	GROUP234

Table 10. Effective Access List with scope (EFFECTIVE, SCOPE modifiers or ACL EFFECTIVE SCOPE)

User	Access	Access List id
USER1	OWNER	USER1
USER1	READ	USER1
USER2	UPDATE	USER2
USER3	NONE	USER3
USER4	READ	GROUP234
USER5	ALTER-O	- oper -

Table 11. Exploded Access List without scope (EXPLODE modifier or ACL EXPLODE NOSCOPE)

User	Access	Access List id
USER1	CONTROL	GROUP12
USER1	READ	USER1
USER2	CONTROL	GROUP12
USER2	UPDATE	USER2
USER2	READ	GROUP234
USER3	READ	GROUP234
USER3	NONE	USER3
USER4	READ	GROUP234
USER4	ALTER-O	- oper -
USER5	ALTER-O	- oper -

Table 12. Trust Access List (ACL TRUST)

User	Access	Access List id
USER1	OWNER	USER1
USER1	CONTROL	GROUP12
USER1	READ	USER1
USER2	CONTROL	GROUP12
USER2	UPDATE	USER2
USER2	READ	GROUP234
USER3	READ	GROUP234
USER3	NONE	USER3
USER4	READ	GROUP234
USER5	ALTER-O	- oper -

An access list can be sorted in three ways:

1. by access level (from ALTER to NONE
2. by userid
3. by access list id (that is, the id on the access list, not the resolved or exploded userid).

In the examples, the access list is sorted by user ID. The ACL display format shown is determined by the combination of the sort order and the access list format, which are independent settings.

The default access list layout can be set on the Setup View Panel (Figure 550 on page 1660) and using the SET primary command. On a display like the User or Data set overview display that has an access list or a connect overview, the layout can also be changed using one of the following ACL primary commands.

ACL NORMAL, or ASIS
Shows the actual access list. That is, the list is not exploded, resolved, or effective with no administrative authorities regardless of whether you add SCOPE or NOSCOPE to the command.

ACL RESOLVE
Shows a resolved access list. It omits administrative authorities unless you add SCOPE to the command.

ACL EXPLODE
Shows an exploded access list. It adds administrative authorities unless you add NOSCOPE to the command.

ACL EFFECTIVE
Shows an effective access list. It omits administrative authorities unless you add SCOPE to the command.

ACL TRUST
Shows the trust relations of the profile. This command shows all ways in which the user currently has data access as well as administrative access. These access entries are the same as the trust relations that are considered for the TRUSTED report types if the profile protects a sensitive resource.

ACL SCOPE
Activates display of administrative authorities as part of the access list display. This command includes group-special authority, and ownership authority through owner and High-level qualifiers. The command is honored only if the access list is not displayed in ACL NORMAL mode.

ACL NOSCOPE
Deactivates display of administrative authorities as part of the access list display.

ACL SORT ID
Sort access list by id

ACL SORT USER
Sort access list by user (with resolve/explode)

ACL SORT ACCESS
Sort access list from OWNER to NONE

ACL UNIVERSAL
Takes system-wide operations and users with a default connection to a universal group into consideration when building the access list. It has no effect on the current SCOPE or NOSCOPE and NORMAL, EXPLODE, RESOLVE or EFFECTIVE settings. The command is refused if only a part of the RACF database has been read.

ACL NOUNIVERSAL
This deactivates the UNIVERSAL option. It has no effect on the current SCOPE or NOSCOPE and NORMAL, EXPLODE, RESOLVE or EFFECTIVE settings.

You can use abbreviations for the ACL commands. For example, you can issue the command `ACL S AC` for `ACL SORT ACCESS`.

If you want to change an access list by typing over the values in the fields, the access list must be in normal mode, `ACL NORMAL` , for example). It can be in any sort order.

IN INFORMATION - Information and documentation

The INFORMATION menu option **IN.M** provides access to an online version of the *IBM Security zSecure: Messages Guide* in IBM BookManager format. This guide provides information about all the messages that can be issued by different IBM Security zSecure products. You can also access the *IBM Security zSecure: Messages Guide* and other zSecure documentation online. For more detailed information, see "Accessing publications online" on page xvi.

For more information about RACF administration and commands, you can refer to the following IBM RACF manuals listed.

- z/OS Security Server (RACF) **Command Language Reference** (SA22-7687) This manual describes all RACF commands, parameters, and options in detail.
- z/OS Security Server (RACF) **Security Administrator's Guide** (SA22-7683) This manual is the primary reference for RACF system and group administrators.

LO LOCAL - Locally defined options

Use the LOCAL option to create customized versions of the IBM Security zSecure panels or to add new functionality to the product. This option is designed to be used by personnel who are experienced in writing ISPF dialogues. For details on using this option see the section on locally defined functions in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

FIELDS - Show CARLa fields available

The primary command FIELDS shows the field names defined in zSecure, as well as those defined in the RACF templates, together with the default properties assigned by zSecure.

You can use the first display that is shown to select either the built-in fields of the product or the fields imported from RACF.

```
zSecure Display Selection                          1 s elapsed, 0.4 s CPU
Command ===> ____________________________________________________ Scroll===> CSR

  Name     Summary Records Title
s BUILTIN       52    2490 Builtin field definitions by newlist type
_ TEMPLATE       1     451 RACF template definitions
****************************** Bottom of Data ********************************
```

Figure 21. Display Selection panel

After selecting the *built-in* fields, a panel is displayed showing all `NEWLIST` types for which *built-in* fields have been defined as shown in Figure 22 on page 36. To view the fields defined for a `NEWLIST`, type a `/` in the entry field for the `NEWLIST` type entry, then press **Enter**. A detail panel opens with a listing of the fields defined for the `NEWLIST` as shown in Figure 22 on page 36.

```
zSecure FIELD summary
Command ===> _____________________________________________ Scroll===> CSR
                                                  25 Mar 2005 14:02
   Type                    T2 Fields Rpt Mod Sub Tag
__ AUDIT                   SA      9                33
__ AUTAB                   AU      9                14
__ CLASS                   CL     64   1   9       12
__ CONSOLE                 CO     33                20
__ CSM                     CM     12                30
__ DASDVOL                 DV     18   9            3
__ DSN                     DS     35   1            2
__ DSNT                    NT     26                15
__ EXIT                    EX     28   1           28
s_ FIELD                   FL     21   2           59
__ IOAPP                   IA     16   2           27
__ JOBCLASS                JC     21               23
__ MEMBER                  MB     51  10           35
__ MERGE                   MR     12   1           37
__ MOUNT                   MN     27               54
__ MSG                     MS     14               21
__ PC                      PC     67  16           19
__ PPT                     PP     14               24
```

Figure 22. FIELD summary panel

This display shows the following columns.

Table 13. Built-in fields available for NEWLIST type

Field name	Description
Type	The name of the NEWLIST type.
T2	The two character abbreviation used to identify the NEWLIST type where a full name cannot be used.
Fields	The number of fields defined for this NEWLIST type.
Rpt	The number of fields with multiple values for one record defined for this NEWLIST type.
Mod	The number of modifiable fields defined for this NEWLIST type.
Sub	The number of fields that can be used for subselect processing, defined for this NEWLIST type.
Tag	A number, identifying this NEWLIST type internally.

```
zSecure FIELD summary                                    Line 1 of 21
Command ===> _____________________________________________ Scroll===> CSR
                                              25 Mar 2005 14:02
   Field                  Description                  Len Format
__ ADVERTIZE              Advertize (do not deprecate)   3 YesNo
__ BASE                   Based on field                 8 Char
__ CASESENSITIVE          Field input case-sensitive     3 YesNo
s_ DESCRIPTION            Field prefix header           29 Char
__ FIELD                  Field name                    24 Char
__ FIELD_TAG              Internal field number (tag)    5 DEC
__ FORMAT                 Default output format         16 Char
__ HEADER                 Default output header         48 Char
__ HELP_PANEL             Field level help panel         8 Char
__ HORIZONTAL             Horizontal repeat group        3 YesNo
__ LENGTH                 Default output length          6 NumVaries
__ LOOKUPONLY             Field only for ID lookup       3 YesNo
__ MAXIMUM_LENGTH         Maximum length on input        6 Dec$blank
__ MODIFIABLE             Field is modifiable            3 YesNo
__ NEWLIST_ABBREV         newlist type 2-letter key      2 Char
__ NEWLIST_TAG            Internal newlist type (tag)    5 DEC
__ NEWLIST_TYPE           newlist type                  24 Char
__ REPEATED               Repeat-group flag              3 YesNo
__ RESTRICT               Output and scope restrictions  9 Char
__ SUBSELECT              Part of subselect group        8 Char
__ WRAP                   Wrapped repeat group           3 YesNo
******************************* Bottom of Data ********************************
```

Figure 23. Field summary - overview display

Table 14 describes the columns available on the FIELD summary panel. You must scroll the display to the right to view some of the fields.

Table 14. Field summary for NEWLIST type **built-in** *field*

Field name	Description
Field	The name of the field.
Description	A short (29 char) description of the field function.
Len	Default output length.
Format	Default output format.
Rpt	Indicates if this field can contain multiple values for one record.
Mod	Indicates if this field can be modified on a display.
Id	Numerical field identifier.
Help pnl	The help panel associated with this field.
Hor	Indicates if the field has the HORIZONTAL modifier by default.
Wrp	Indicates if the field has the WRAP modifier by default.
Lwr	For modifiable fields, this field indicates if mixed case input is accepted. For non-modifiable fields, the field is empty. Modifiable fields are only available with a zSecure Admin entitlement.
SubSelct	Shows the names of the repeated fields that can be used with this field in subselect processing.
Restrictions	This shows the authority that a user needs to see this field when running in restricted mode.
Header	The default header.

When you select one of the fields on this display you are shown the following detail panel. This panel contains the same information, but it is shown in a more expansive format.

```
zSecure FIELD summary                              Line 1 of 23
Command ===> _____________________________________ Scroll===> CSR
                                                 25 Mar 2005 14:02


  newlist type
  newlist type                  FIELD
  newlist type 2-letter key     FL
  Internal newlist type (tag)   59
  Field definition
  Field name                    DESCRIPTION
  Field prefix header           Field prefix header
  Part of subselect group
  Default output format         Char
  Default output length         29
  Default output header         Description
  Maximum length on input
  Based on field
  Repeat-group flag             No
  Field is modifiable           No
  Horizontal repeat group       No
  Wrapped repeat group          No
  Field input case-sensitive    No
  Internal field number (tag)   7
  Field level help panel        C2R3FL07
  Output and scope restrictions
****************************** Bottom of Data ********************************
```

Figure 24. Field summary - detail display

XML support within IBM Security zSecure

XML has become the standard for cross-platform and intersystem communication. IBM Security zSecure can transform your system data, security controls, and event (SMF) reports to make the best use of XML for your applications.

First some definitions:

XML (eXtensible Markup Language)
A language composed of labels and values. The values are grouped in a context and can be represented as a tree.

DTD (Document Type Definition)
The syntactic definition of the XML document, which is used to determine the validity of the document. The DTD contains a basic description of each element by describing its general format, identifying its possible attributes, and detailing its repeatability. The DTD can be internal to the document or externally referenced.

XSLT (eXtensible Stylesheet Language Transformations)
A standardized XML-based collection of commands, also called a vocabulary or markup language, to transform the content and data stored within an XML document into a different form. An XSLT is referenced within the document that is to be transformed. zSecure provides a default stylesheet zSecure provides a sample XSLT stylesheet available at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.13/c2rxsl01.xsl. For details, see "The XML_STYLESHEET parameter" on page 41.

An XML document is a file or data set with tags defining its content but not its format. This separation between content and format means that the same document can be processed with different XSLT styles sheets to produce different output. For example, an XML document can be processed against one XSLT

stylesheet and produce an HTML file for display by a browser. That same XML document processed against a different XSLT stylesheet can produce a differently formatted report suited for display on a wireless device, and a third stylesheet might produce input appropriate for Microsoft Excel. There is no limit to the number of layouts that can be produced by the same XML document by applying different XSLT files. The real power of this becomes apparent with the realization that, because the data (XML document) is independent of the format (XSLT file), the input files can change, but as long as the document conforms to the DTD, it can be transformed by any XSLT file utilizing the DTD for the document.

These three files (XML, DTD, and XSLT) work together to produce a self-documenting database system readable by any platform or system recognizing XML. There are no proprietary data formats, as there are with most contemporary database systems. This means that any machine based (or human based) process can read and understand the basics of the data.

There is a fourth piece of the report output which is specific to zSecure. It is a data dictionary which, if requested, is embedded within the generated document and assists the XSLT in formatting the XML document. The data dictionary is required for any XML reports requesting the default XSLT be used to format the output. The data dictionary is optional if the default XSLT is not used.

Although XML is generally used for B2B processes, it can also be used within an enterprise. For example, an zSecure XML report can be routed to a browser for display, or it can be viewed by other programs such as Microsoft Excel and other XML services using the XSLT to transform the data.

Starting with IBM Security zSecure

zSecure produces XML output instead of the usual text output by changing a few options in the zSecure program requesting the report.

The first step is specifying `FILEOPTION FILEFORMAT=XML`. By this specification, several new rules come into play:

1. The `NEWLIST` statements must be named because these names are used as an `ELEMENT` in the XML document. Names must conform to both zSecure and XML standards.
2. There must be no duplication of field names in a `LIST` statement with the ddname, `NEWLIST`, and `MERGELIST` names. This requirement makes each of these entries unique and avoids confusion.
3. The implementation used for XML rules in zSecure also requires that field names be unique within a `LIST` statement. Users cannot display or report the same field more than once per `LIST` statement. However, if there is a need to do so, users could use a `DEFINE` statement to provide the field with a different name.
4. Ensure that the output file is not used by any other (non-XML) support functions. Do not reference the file before the `FILEOPTION` command that indicates its use as an XML file.
5. All field names, `NEWLIST` names, and ddnames must use the following conventions:
   a. Contain only alphabetic or numeric characters, underscores, or hyphens, and no national characters (#$@).
   b. Begin with an alphabetic, but not the character string: XML.

The ddnames have an additional limitation: The names must not contain hyphens or underscores.

In its simplest form, the data report contains only one element per NEWLIST statement. Without any additional parameters the output is the header and values, as shown in Figure 25. Most applications generate more comprehensive reports with many more entries. To display these reports, it is probably best to use XSLT to transform the document.

By default, an inline DTD is included in the output. If NOXML_DTD or an imbedded XSLT stylesheet is requested, the DTD is suppressed. Using a DTD provides a self-documenting XML document and enables XML parsers to validate the document.

Without an XSLT to tell the using program how to format the document, web browsers, Excel and other programs are able to parse the XML document in a simple layout, without any special formatting. You must allocate an output dataset to MYXML before running this sample report in batch or ISPF.

```
fileoption  dd=myxml fileformat=xml
newlist dd=myxml type=system name=SYS
sortlist system mvslvl
```

```
<?xml version="1.0" encoding="IBM1047"?>
<!DOCTYPE MYXML [
<!ELEMENT MYXML (SYS)*>
<!ATTLIST MYXML
     creation CDATA #REQUIRED
>
<!ELEMENT SYS (SYSTEM?, MVSLVL?)>
<!ELEMENT SYSTEM (#PCDATA)>
<!ELEMENT MVSLVL (#PCDATA)>
[>
<MYXML creation="2007-04-18T04:01:41.88+02:00">
<SYS>
<SYSTEM>DEMO</SYSTEM>
<MVSLVL>SP7.0.4</MVSLVL>
</SYS>
</MYXML>
```

Figure 25. Two cells in table: zSecure input - XML text output when browsed (via ISPF) on the mainframe

Use XSLT and the data dictionary to format the output

The power of XML becomes more apparent with the zSecure option to generate a processing instruction to use an XSLT stylesheet.

The XSLT supplied with zSecure produces a tabular report that can be used by web browsers, Microsoft Excel, and other such programs. However, if you want different formatting, you can define and apply your own XSLT.

After specifying two additional FILEOPTION parameters: XML_STYLESHEET and XML_DATADICT, the example document grows to 309 lines. This is because the new document includes the zSecure default XSLT stylesheet together with the data dictionary. The data dictionary is required only when using the default stylesheet provided with zSecure.

The data dictionary is valuable as it provides information about the report title, top title, and subtitle as well as vital formatting information for each field in the report. This information is used by the stylesheet to format the report as seen in Figure 26 on page 41.

Figure 26 also illustrates how to output the XML document into an existing z/OS data set using the XML_DATADICT parameter. This option is useful if the document is to be used in a zSeries® processing environment.

```
alloc dd=myxml dsn=user1.output.xml type=output
fileoption dd=myxml encoding=EBCDIC fileformat=xml xml_datadict,
       xml_stylesheet=imbed(m=c2rxsl01)
newlist dd=myxml type=system name=SYS
 list system mvslvl
```

```
0001 <?xml version="1.0" encoding="IBM1047"?>
0002 <?xml-stylesheet type="text/xsl" href="#"?>
0003 <xsl:stylesheet id="C2RXSL01" version="1.0"
0004     xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
. . .
0299 <field name="MVSLVL" format="" width="8" align="left">
0300 <header>MVS</header><description>MVS level</description>
0301 </field>
0302 </report>
0303 </datadict>
0304 <SYS>
0305 <SYSTEM>DEMO</SYSTEM>
0306 <MVSLVL>SP7.0.4</MVSLVL>
0307 </SYS>
0308 </zAudit:MYXML>
0309 </xsl:stylesheet>
```

Figure 26. Two cells in table: zSecure input - XML text output. Note that lines 299-301 show the result of specifying the XML_DATADICT parameter

If you change the `dsn=user1.output.xml` option to a fully qualified z/OS Unix path, the output can be routed to a file in your HFS or zFS file system. The z/OS UNIX file is created if it is not present when needed. However, the directory path must exist. The code for this example is shown in Figure 27.

```
alloc dd=myxml type=output path='/u/user1/work.xml'
fileoption dd=myxml fileformat=xml xml_datadict,
       xml_stylesheet=imbed(m=c2rxsl01)
newlist dd=myxml type=system name=SYS
 sortlist system mvslvl
```

Figure 27. Outputting XML to z/OS Unix file

The XML_STYLESHEET parameter

The XML_STYLESHEET parameter allows different style sheets to be specified, providing maximum flexibility. You can request that it be included within the document by specifying `XML_STYLESHEET=IMBED(optional_ddname,membername)`. As previously seen in Figure 26, this parameter increases the size of the document. Instead, it can be preferable to specify the location of the stylesheet using the `URI` parameter. The `URI` parameter accepts the standard Uniform Resource Identifier for the stylesheet specification, for example http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.13/c2rxsl01.xsl. When the stylesheet is specified by `URI` parameter, the stylesheet is not embedded which makes the document much smaller. However, the `URI` option does require that the user have access to the resource referenced in the URI.

The `IMBED` option enables a local style sheet while the `URI` enables the installation to use a centralized production stylesheet. The local option is useful to develop and test the stylesheet in a test environment, and the `URI` option is useful for using proven stylesheets in the production environment. You can also specify the `URI` option for internal users that have access to the file or data set specified by the `URI` file/data set), and use the `IMBED` option for shipping to external users where it is not practical to provide public access to a `URI` file or data set. Alternatively, you

might want to have test and production versions within the IMBED or URI parameters as well.

```
alloc dd=myxml dsn=crmbmh1.output.xml type=output
fileoption dd=myxml  fileformat=xml xml_datadict,
  xml_stylesheet=URI('http://publib.boulder.ibm.com/infocenter/
                     tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.12/c2rxsl01.xsl')
newlist dd=myxml type=system name=SYS
 sortlist system mvslvl
```

Figure 28. Use of the URI= parameter for the stylesheet specification

The power and flexibility provided by these parameters is important.

1. By having the DTD included within the document, validating the document is easier, and changes to the report do not cause invalid documents to be created. The document is also self documenting since it carries its own basic definitions.
2. Using the default stylesheet makes it effortless to produce tabular format reports that can be viewed by programs that process HTML documents.
3. Total flexibility with regards to the stylesheet specification makes it simple for an installation to tailor and use a customized stylesheet with minimal effort. The only requirement is to change the URI value or specify the IMBED parameter.

Output Processing

Output preparation is also important. XML output lines can be longer than most people expect. Ensure that your mainframe output file is defined with RECFM=VB and a large LRECL. For example, LRECL=255 is an acceptable value for testing, but for production use, a larger number, such as 1024 is preferable. As shown in Figure 27 on page 41, z/OS Unix files in your HFS or zFS file systems are also appropriate destinations for your XML reports.

Optimal encoding of your output differs by the system on which it is processed. By omitting the ENCODING parameter on the FILEOPTION statement, it defaults to EBCDIC, which is appropriate for mainframe usage. However, if you plan to display the output on a PC, we recommend that you specify ENCODING=UTF-8 (Unicode). If you transfer a mainframe formatted XML document to the PC, the ENCODING parameter value can cause parsers to issue a diagnostic error. To prevent this problem, remove or replace the encoding="IBM1047" with the proper encoding value.

zSecure runs on zSeries mainframes, but there are many means of distributing the resulting output. In addition to the traditional FTP mechanisms, zSecure offers a few options within itself. The output can also be routed through the zSecure email interface, once it has been set up, when coupled with the OUTPUTFORMAT=ATTACH parameter.

```
fileoption dd=c2remail fileformat=xml xml_datadict,
       xml_stylesheet=imbed(m=c2rxsl01) encoding=utf-8
option dd=c2remail mailto=user1@company.com,
       from=user2@company.com  outputformat=attach
newlist dd=c2remail type=system name=SYS
 sortlist system mvslvl
```

Figure 29. Configuring the zSecure request to email the output as an attachment

After the zSecure program in Figure 29 runs (either batch or ISPF), the email is sent with the attached file. Remember that other email options, such as REPLYTO=, are also available for your use.

Attaching documents adds another powerful feature to the zSecure XML support: You can email the report document from the mainframe to the recipients. Then, they can review the file using the program of their choice, at their convenience.

If you decide to transfer the XML file from the mainframe to a PC using FTP or another such transport mechanism, remember to consider the file encoding. If the report was originally produced with no `ENCODING` or `ENCODING=EBCDIC`, it must be transferred as a CHAR operation. However, if the report was produced with the PC in mind, with `ENCODING=UTF-8`, it must be transferred as a BINARY operation. Normally, UTF-8 data is not displayable on the mainframe without UNICODE processing. One other caveat, converting EBCDIC to ASCII (as in a CHAR transfer) cannot handle the '[' and ']' characters in XML properly.

SUMMARY Reports and XML

When the default XSLT is applied to the zSecure SUMMARY reports they are formatted just like the printed zSecure report. The SUMMARY report produces rows of output, omitting the repeated values of the leftmost fields and providing values for the fields on the rest of the row.

The sample program in Figure 29 on page 42 runs on the mainframe and e-mails the output to the specified user who then can review the output using Notepad, a web browser, Microsoft Excel, or another XML formatting program. For samples of the program and output, see the following figures.

```
fileoption dd=c2remail fileformat=xml xml_datadict,
       xml_stylesheet=imbed(m=c2rxsl01) encoding=utf-8
option dd=c2remail mailto=user2@company.com,
       from=user1@company.com outputformat=attach
newlist dd=c2remail type=smf name=allomvs
 select event=allomvs
 summary userid * event
```

Figure 30. IBM Security zSecure program to email SUMMARY report information

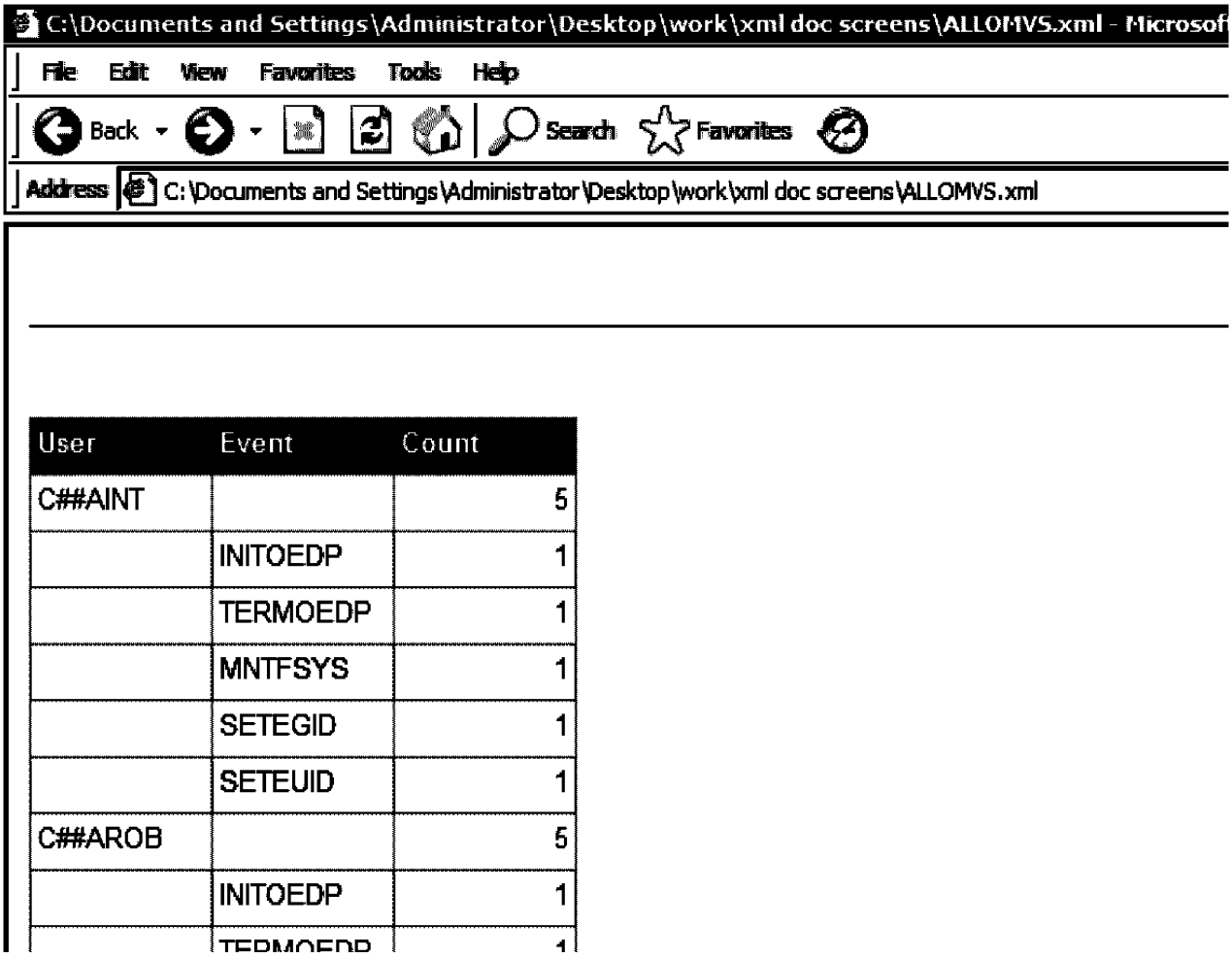
```
******************************** Top of Data ********************************
S M F   R E C O R D   L I S T I N G   24Apr07 17:41 to 26Apr07 15:01

User     Event    Count
C##AINT                5
         INITOEDP       1
         TERMOEDP       1
         MNTFSYS        1
         SETEGID        1
         SETEUID        1
C##AROB                5
         INITOEDP       1
         TERMOEDP       1
         MNTFSYS        1
         SETEGID        1
         SETEUID        1
******************************** Bottom of Data ********************************
```

Figure 31. SUMMARY report: Plain text output

```
<zSecure:C2REMAIL creation="2007-05-02T17:24:59.49+02:00" xmlns:zSecure="http://www.ibm.com/">
<datadict>
...
</datadict>
<ALLOMVS>
<USERID>C##AINT</USERID>
<Count>5</Count>
</ALLOMVS>
<ALLOMVS>
<EVENT>INITOEDP</EVENT>
<Count>1</Count>
</ALLOMVS>
<ALLOMVS>
<EVENT>TERMOEDP</EVENT>
<Count>1</Count>
</ALLOMVS>
<ALLOMVS>
<EVENT>MNTFSYS</EVENT>
<Count>1</Count>
</ALLOMVS>
<ALLOMVS>
<EVENT>SETEGID</EVENT>
<Count>1</Count>
</ALLOMVS>
```

Figure 32. SUMMARY report: Raw (unformatted) XML



User	Event	Count
C##AINT		5
	INITOEDP	1
	TERMOEDP	1
	MNTFSYS	1
	SETEGID	1
	SETEUID	1
C##AROB		5
	INITOEDP	1
	TERMOEDP	1

Figure 33. SUMMARY report: Microsoft Internet Explorer format

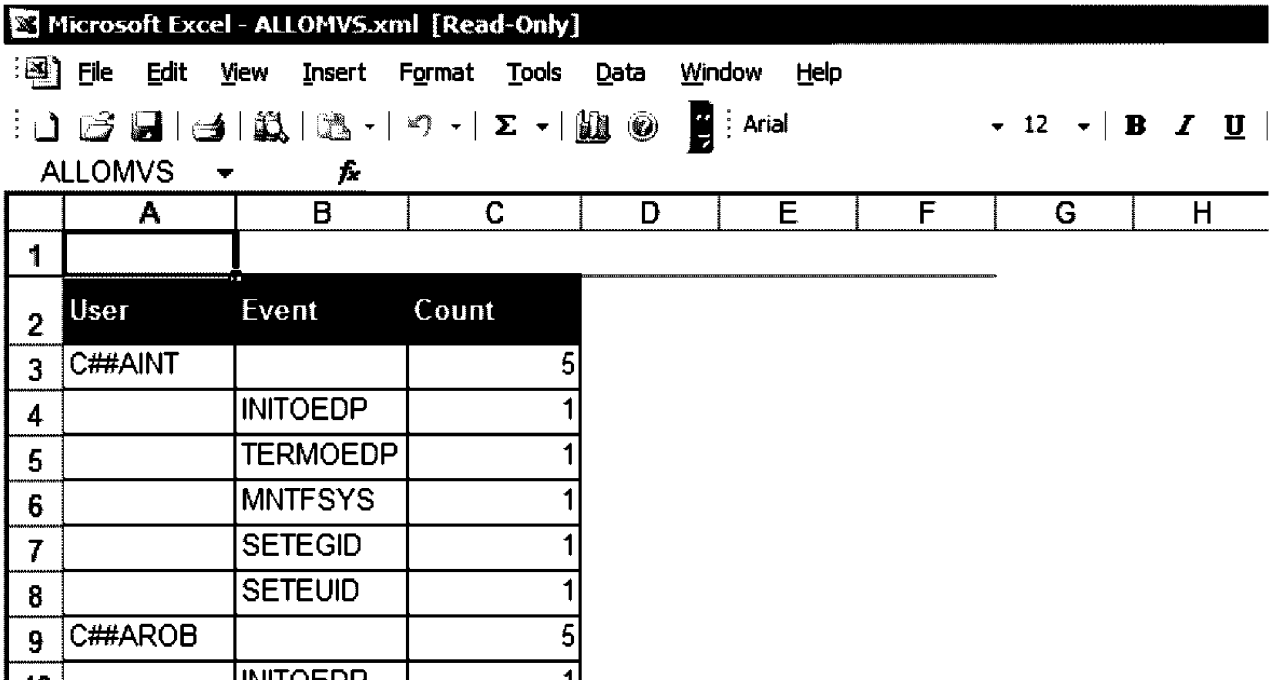


Figure 34. SUMMARY report: Excel format

XML-proofing zSecure reports

You can produce XML output from some of the existing (tabular output) sample zSecure reports by adding the necessary XML parameters to the OPTION, FILEOPTION, or NEWLIST commands before the INCLUDE command which imbeds the report program. Other zSecure reports produce formatted reports with inserted text or output which is not in tabular format, or they produce ISPF displays. These reports do not work if an attempt is made to convert their output to XML. The WRAP formatting option is also not available when the output is going to XML.

Finally, as you adapt your existing zSecure reports to the XML capability, remember to observe the requirements detailed in Section "Starting with IBM Security zSecure" on page 39.

Summary

XML output provides reports that can be utilized in multiple fashions using XSLT. zSecure provides XML output when the proper output parameters are specified. The DTD is generated by default, unless the `XML_STYLESHEET=(IMBED(membername))` option is specified. `XML_DATADICT` is required if the IBM-supplied default XSLT is specified.

Names of fields, `NEWLIST` types, and ddnames have limitations and must contain only alphabetic and numeric characters, underscores, or hyphens. National characters (`#$@`)) are not supported. The value must begin with an alphabetic character but not the string XML. The ddnames cannot contain hyphens and underscores.

Ensure the z/OS output data set is allocated with VB record format and a large LRECL (for example 1024). The default encoding is `EBCDIC` for mainframe usage

and UTF-8 for PC usage. This default is used if the ENCODING= parameter is omitted. Use of email services can simplify transfer to PCs by using the email operands and OUTPUTFORMAT=ATTACH.

Output formatting can use the IBM-supplied default or an installation-defined XSLT. The XSLT can be embedded or referenced by web address in the URI parameter.

Conclusion

zSecure supports the generation of XML documents from system data. These documents can be transformed to commonly used formats such as Microsoft Excel and other formats to meet the needs of the organization and users. This functionality is provided in addition to zSecure support for generate letters from the information provided in SMF event reports and security database fields. With the XML support, zSecure can use different style sheets to provide the security administration and auditing information from a single XML report in multiple output formats and for viewing on multiple output devices such as cell phone, pagers, and email.

Compare processing

Use compare processing to detect and report on changes in selected fields by comparing the values in a designated baseline CKFREEZE data set against another CKFREEZE data set.

For an example of how the compare process is used, see the *IBM Security zSecure Alert: User Reference Manual* for information about the zSecure Alert extended monitoring function. This function performs a comparison that monitors system settings and reports changes using the Alert messaging function.

You can set up your own compare process using the CARLa language statements and options for compare processing. The comparison process is described in "Setting up and running a comparison."

Setting up and running a comparison

Use the COMPAREOPT statement to define a set of comparison properties for any NEWLIST that references it using the COMPAREOPT=name option.

Figure 35 on page 47 provides an overview of setting up and processing a comparison. To understand the process description that follows the diagram, review the following terms.

COMPARE_CHANGES
Defined variable type for listing the differences in the fields that are compared. See "Defining variables for comparison results (COMPAREOPT)" on page 754.

COMPARE_RESULT
Defined variable type for returning a value that describes the outcome of the compare process. For example, if the compare results show a new item, ADD is returned. If a value has been modified, the value CHG+ is returned. See "Defining variables for comparison results (COMPAREOPT)" on page 754.

COMPAREOPT
The CARLa statement that specifies the compare options which determine what to compare.

BY=
Specifies the value for the key used in the comparison process to determine the set of records to be compared. This parameter is specified in the `COMPAREOPT` statement.

BASE=
Specifies the condition that designates the baseline record in the set specified using the `BY=` parameter.

COMPARE=
Determines the list of fields to be compared. This parameter is specified in the `COMPAREOPT` statement.

SHOW=
Determines which of the compared records to include in the output based on the `COMPARE_RESULT` value returned. This parameter is specified in the `COMPAREOPT` statement.

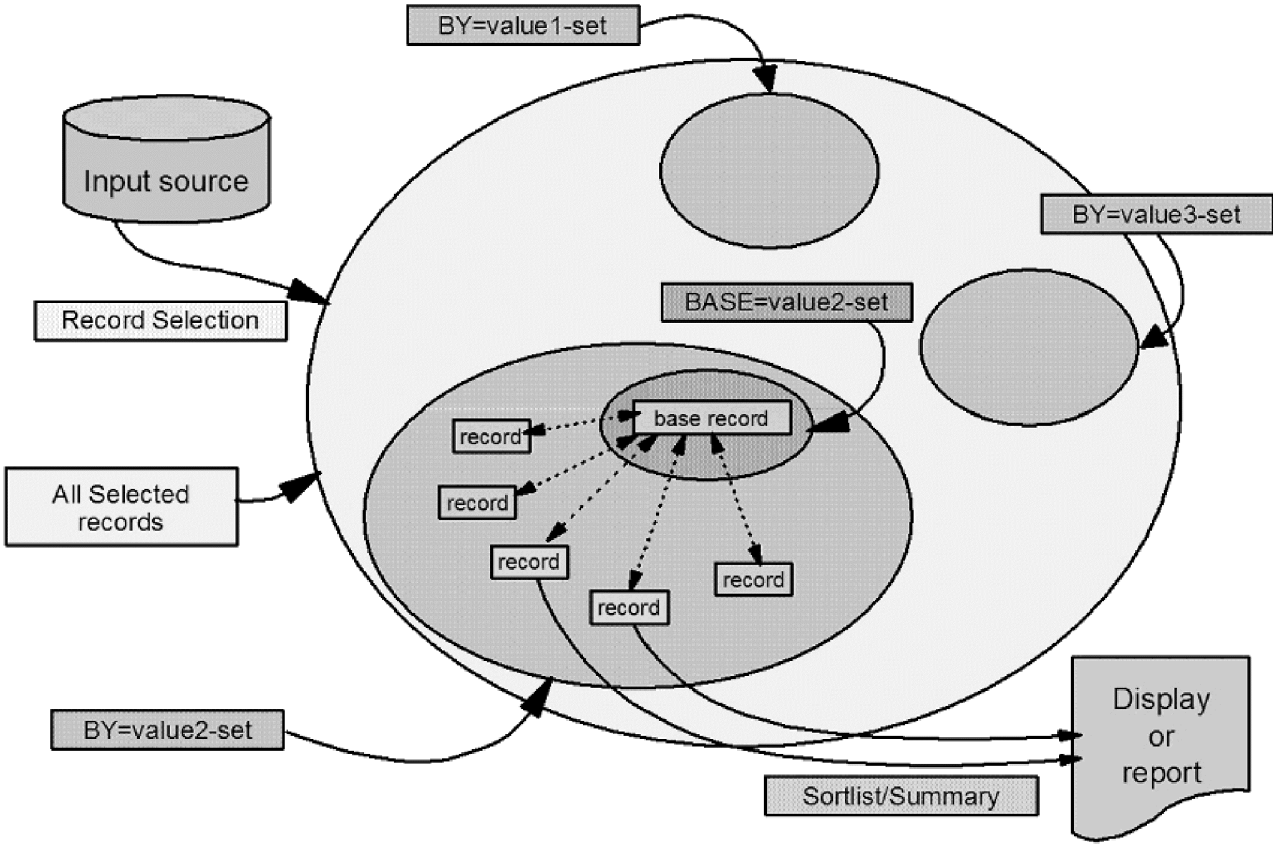


Figure 35. Compare processing conceptual diagram

When compare processing is activated, the `CKRCARLA` program uses the standard select and exclude processing to read the required data from the applicable input source. The read operation creates an in-memory data structure representing the input data. In the process diagram, this structure is shown as *All Selected records*. Conceptually, *All Selected records* is the population to be compared. The comparison process works on subpopulations. All records that share the same `BY` values are considered to be a subpopulation. Only records that have the same `BY` values are

compared. Other records that have a disjunct set of BY values are part of other subpopulations that are also compared internally.

Within the subpopulation, one or more records are identified by the BASE specification. Ideally, this is a single record, but it can also be a set of several records. If this is a single record, it is called the baseline record. If the BASE specification does not identify a single record, one of the records from the BASE set is selected to be the baseline record. For information about how a record is selected as the baseline, see "Selecting the baseline record."

Within the subpopulation, all records are compared against the baseline record. The comparison is done only for the fields explicitly selected using the COMPAREOPT specification. All other fields are ignored for the compare processing. The result of the comparison operation is one of the COMPARE_RESULT values which provides information about the type of change. For example, a COMPARE_RESULT value can be ADD if the field was added, or CHG if the field value changed. The results can also indicate whether a change resulted in an increase or decrease in the level of security compliance. (See "Defining variables for comparison results (COMPAREOPT)" on page 754.

If the COMPARE_RESULT matches the SHOW specification, the record is kept. If the COMPARE_RESULT does not match the SHOW specification, the record is discarded, which results in a reduced subpopulation.

If the output specification (SORTLIST or DISPLAY) for the record contains a variable defined as COMPARE_CHANGES, the variable is updated to include the changed fields that are selected by the SHOW specification.

The next stage of the compare process is the summary. This stage uses the standard summary process that works on the reduced population (that is, the combination of all reduced subpopulations). The summary processing uses the summary variables as defined in the summary statement.

Selecting the baseline record

If the BASE specification does not result in a single record within the subpopulation, an arbitrary record is selected to be the baseline record. This selection is based on the fields specified on the sortlist and summary statements in this NEWLIST. The record with the lowest field value in the sequence as defined by the sortlist and summary fields is used. If multiple records have the same values for all listed fields, an arbitrary record is chosen. The record selected is not important because the difference is not visible.

No direct relationship exists between the record key that uniquely identifies the record, the list of BY fields, or the list of fields used for summary processing. However, if no list of BY fields has been specified, the program uses a default set of BY fields that resembles the unique record key.

Creating the DEFAULT COMPAREOPT specification

zSecure includes a pre-defined COMPAREOPT specification with the name DEFAULT that can be used to trigger default compare processing when the COMPAREOPT specification is not explicitly defined using the COMPAREOPT statement. This default specification is established using the ALLOC FUNCTION BASE*name* option without specifying a complex name.

The DEFAULT COMPAREOPT specification is equivalent to specifying the following COMPAREOPT statement:

```
COMPAREOPT NAME=DEFAULT TYPE=<anything> BASE=(COMPLEX=complex) SHOW=DIFF
```

Note: Because the DEFAULT specification applies to multiple NEWLIST types, this COMPAREOPT specification cannot be entered as a valid CARLa statement. It is only shown here to illustrate what is specified by the default.

The default COMPAREOPT specification does not specify values for BY and COMPARE. The default specifications are used for these parameters. (See "Selecting the baseline record" on page 48.)

Use of the FUNCTION=BASE specification is not required. It is used to trigger default compare processing. Explicit compare processing using the COMPAREOPT parameter on the NEWLIST statement is possible without any FUNCTION=BASE specification.

For more information, on the syntax and processing considerations, see the FUNCTION=BASE parameter in "Explicit allocation mode" on page 720.

Setting up the CARLa language input for compare processing

Table 15 provides a summary of the statements and formatting options that you can use to setup a compare process. For more detailed information about any of the resources, see the links included in the process description fields.

Table 15. CARLa commands, options and output formats for compare processing

CARLa command, option, or output format	Description
COMPAREOPT statement	This CARLa statement specifies what is to be compared in a comparison process. After the COMPAREOPT specification has been created, the compare process it defines can be run for supported NEWLIST types. See "COMPAREOPT" on page 739.
ALLOCATE FUNCTION=BASE	Use this option to specify a default baseline data set to be used for compare processing. If no explicit COMPAREOPT statements are defined, this baseline data set is used. The FUNCTION=BASE specification is not required for compare processing. However, it can be used to trigger default compare processing when no explicit COMPAREOPT statement has been defined. See the FUNCTION=BASE parameter description in "Explicit allocation mode" on page 720.
NEWLIST COMPAREOPT=compareopt	The COMPAREOPT keyword on the NEWLIST statement specifies the name of the COMPAREOPT statement to be used for the NEWLIST. See "NEWLIST" on page 846.
OPTION COMPAREOPT=compareopt	The COMPAREOPT=compareopt parameter for the Option command designates a default COMPAREOPT statement to be used for all newlists that do not explicitly specify a COMPAREOPT name. You can specify DEFAULT for the compareopt value to use a system-defined default COMPAREOPT specification. See "OPTION" on page 856.
DEFINE COMPARE_RESULT COMPARE_CHANGES	These defined variable fields are used to output the results of a compare operation that includes information about changed fields and a security compliance status indicator that indicates how the change impacted the level of security compliance. The field values included in the output depend on the options specified in the COMPAREOPT statement. See "Defining variables for comparison results (COMPAREOPT)" on page 754.
Output formats	For information about formatting options for the results of a compare operation (COMPARE_RESULT), see "COMPARE processing output formats: Formatting COMPARE_CHANGES results" on page 829.

Chapter 2. RACF Administration Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

General information

The interactive component of Security zSecure is an ISPF application available under MVS/TSO.

For details on how to start this component, see "Starting the interactive component" on page 9. For information about the ISPF panels in the product, see "Panel structure" on page 10.

Use the **RA RACF** option from the main menu to open the RACF administration menu shown in Figure 36.

```
Menu         Options       Info     Commands     Setup
_____________________________________________________________________________
                      zSecure Admin+Audit for RACF - Main menu
Option ===> _____________________________________________________________________
                                                                        More      +
SE   Setup           Options and input data sets
RA   RACF            RACF Administration
  U    User            User information
  G    Group           Group information
  D    Data set        Data set profiles
  R    Resource        General resource profiles
  S    Settings        Setropts, RRSF, and class settings
  H    Helpdesk        One-panel helpdesk options
  Q    Quick admin     Quick User Administration
  1    Access          Access Check
  2    Queued          Display and action on profiles with QUEUED commands
  3    Reports         Reports with profiles and resources
  4    Mass update     Specify mass copy/recreate/delete actions
  5    DIGTCERT        Work with digital certificates
  C    Custom          Custom report
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
 X   Exit            Exit this panel
```

Figure 36. The RACF administration menu

For more information, see the following topics:

- "Performing RACF Administration tasks from the menu" on page 52
- "Using the RACF administration panels" on page 52
- "Line commands" on page 54
- "Managing the Access List display panel" on page 81
- "REFRESH - Automatic refreshes for RACLIST, GENERIC checking, GLOBAL access checking, and WHEN(PROGRAM)" on page 86

Performing RACF Administration tasks from the menu

Table 16 describes the options available for RACF administration.

Table 16. RACF Administration Menu option descriptions

Option	Description
"RA.U USER - User information" on page 87	Creates general ISPF display panels showing information about all or selected user profiles.
"RA.G GROUP - Group information" on page 117	Creates general ISPF display panels showing information about all or selected group profiles.
"RA.D DATASET - Dataset profiles" on page 132	Create general ISPF display panels showing information about all or selected DATASET profiles. This option is only applicable to auditing RACF databases on a z/OS system.
"RA.R RESOURCE - General Resource profiles" on page 147	Creates general ISPF display panels showing information about all or selected general resource profiles.
"RA.S SETTINGS - SETROPTS and class settings" on page 172	Creates display panels showing information about the SETROPTS settings and the Class Descriptor Table.
"RA.H HELPDESK - One-panel help desk options" on page 177	Opens the one-panel Help desk interface for administrative tasks like resetting passwords, resuming users and using CKGRACF scoping.
"RA.Q QUICK ADMIN - Quick User Administration" on page 179	Opens the three-panel Quick Admin interface for administrative tasks like resetting passwords, resuming users and using CKGRACF scoping.
"RA.1 ACCESS - Access Check" on page 184	Research user and group access level to data sets or resources.
"RA.2 QUEUED - Queued commands" on page 185	Work with queued commands
"RA.3 Reports - Reports with profiles and resources" on page 193	Create printed or online, interactive reports for day-to-day maintenance tasks. zSecure provides sample reports that you can use to design and create custom reports for your site. For information, see "Predefined CARLa scripts" on page 251.
"RA.4 MASS UPDATE - Specify mass copy/recreate/delete actions" on page 233	Perform day-to-day maintenance on groups of profiles.
"RA.5 DIGTCERT - Work with digital certificates" on page 244	Manage digital certificates.
"RA.C CUSTOM - User Defined Display (Custom Display)" on page 249	Use a template to design your own query panel in ISPF.

Using the RACF administration panels

When you perform RACF administrative tasks using zSecure, you use several different types of ISPF panels. The options available on the panels and the methods for using fields and running commands can be different depending on the type of panel you are viewing. Review the following information to learn about the panels, fields, and the selection and viewing options.

Panel types. Depending on the suboption you select from the menu, the resulting ISPF display panel can be a standard display panel or a report display panel. The type of display panel determines the available operations. For example, the line commands available on a report display panel are different from the commands available on a standard display. For more information, see "Line commands" on page 54.

When multiple complexes are selected with the `SETUP` files and `SETUP VIEW` option, the option **Add summary to RA displays for multiple complexes** is selected. As a result of this selection, a summary showing the profile differences is added to the **RA.U**, **RA.G**, **RA.D**, and **RA.R** display panels.

- For text fields, the text is shown when it is identical for the selected profiles. When the profiles are different, the text is shown with a common prefix followed by `>`, the text `<more>`, or `+ *` depending on the column width.
- For flag fields, the percentage of true conditions is shown.
- For date fields, depending on the field, the newest or oldest date is displayed. For example, the oldest date is shown for the profile creation date while the newest date is shown for the password change date.

Another type of panel in the product is a selection panel. Use selection panels for specifying the criteria to select information from a data source for review and analysis in zSecure. Only profiles that match all criteria are selected. That is, the effect of a query is to combine the conditions with AND logic before selecting data.

Field processing and filters. If you leave a field in a panel blank, the field is not tested. Fields on selection panels can contain literals or filters, although not all fields accept filters. The following special characters are supported in filters:

Table 17. Filter characteristics

Filter Code	Description
%	Matches any one non-blank character.
*	Matches up to eight characters in the key of a DATASET profile, or any number of characters in one qualifier in other places.
.**	Matches any numbers of qualifiers at the end of a profile name.
:	Searches for the specified substring anywhere in the field. This function is not supported in profile keys, class names, and data set qualifiers.

Viewing details and printing information. In an ISPF display panel, you can generally select rows from the table to display additional information. You can use the primary command PRT or PRTLIST to create a hardcopy of the tables displayed, written to the standard ISPF LIST data set; you can print the ISPF LIST data set from any ISPF panel by issuing the LIST primary command.

Changing field values. If you use zSecure Admin or IBM Security zSecure Admin and Audit for RACF, you can use modifiable fields. This functionality is not available if you only use zSecure Audit. Modifiable fields are fields that you can update. These fields are also referred to as *overtypeable* fields. Profile display fields that you can type over are shown padded with underline characters. You can specify a different character indicator from the ISPF primary menu (option **0 Settings**). The ability to modify fields is a system-defined setting. Use the MODIFY command to turn this function on and off. Additional display options like confirmation level for commands generated, can be set using the SET command.

Line commands

Commands can be generated by typing over a field or by issuing a line command at the start of a line. The line commands available on an ISPF panel depend on the information shown (NEWLIST type) and the profile type such as user profile or DATASET profile (ENTITY type). In addition, the commands specific to zSecure Admin are only supported if that product is installed and active along with zSecure Audit.

For more information, see the following topics:

- "Determining which line commands are available"
- "Standard line commands"
- "Line commands on profile displays" on page 55
- "Line commands on detail displays" on page 74
- "Line commands on non-profile displays" on page 80
- "Line command status messages" on page 80

Determining which line commands are available

In any profile level display, type / in the input entry field. Then, press **Enter** to view a list of the available line commands and their associated functions.

Standard line commands

Documentation for the line commands available on specific RACF profile display panels for user, group, DATASET, and general resource profiles are listed in the documentation for each profile type. To access this information, see the "Performing RACF Administration tasks from the menu" on page 52. Most other profile level displays, such as specific reports, provide the standard line commands listed in Table 18.

Table 18. Standard line commands

Line command	Meaning
/	Type / in an input entry field and press **Enter** to view a list of the line commands available in the current program context.
B	Browse a data set. This command is only valid for non-VSAM data set objects.
C	Copy the profile. The processing for the copy operation depends on the profile type: • If the copy action is for a data set, connect, or general resource profile, running the **C** line command issues a RACF **COPY** command. • For user and group profiles, running the **C** line command issues a Security zSecure command. These commands are always queued in the CKR2PASS file for later execution. Before the command is run or queued, you are prompted with a panel to edit the profile name.
D	Delete the profile. Depending on the profile type, this issues a RACF command (data set, connect, and general resource profiles) or a Security zSecure command (user and group profiles). Security zSecure commands are always queued in the CKR2PASS file for later execution.
L	Issue a LIST command for a DATASET profile, LISTDSD for example. Use this command for reviewing profile status in the active RACF database.
S	Show detail information for the selected profile.

Line commands on profile displays

The following line commands are available on profile displays.

A - Authorizations of a user or group

Use the **A** line command to find the authorizations defined for a user or group. It can only be issued on user or group profiles on profile displays.

This command starts option **RA.3.4** PERMIT/SCOPE for the user or group it is issued for. See "RA.3.4 Permit/Scope - Report access of a user or group" on page 207.

AC - Access

Use the **AC** line command to find the access defined for a user or group on a specified profile. It can be issued on any profile on profile displays.

It opens option **RA.1** ACCESS for the profile it is issued for. For details, see "RA.1 ACCESS - Access Check" on page 184.

This command is only supported if zSecure Admin is installed and active.

C - Copy

Use the **C** line command to copy a profile through a recursive query. For users and groups, you can also use this command for copying ID-specific DATASET, resource profiles, and catalog aliases if a `CKFREEZE` data set with a master catalog dump is provided. For more information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*

This command is only supported if zSecure Admin is installed and active.

For DATASET or resource profiles you can also issue a RACF command to copy from a profile directly or create a temporary profile. If you have an active RACF database allocated, the latter two options open the newly created profile immediately. For temporary profiles, specify either the date of removal, or a number of days after which the profile is to be removed by the daily `CKGRACF` job. (See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.) An optional reason for the temporary profile can be specified as well.

Apart from creating new profiles you can also use this function to copy connect definitions and permits to an existing user or group.

The panel it starts for a group is shown in Figure 37 on page 56.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Copy
Command ===>_____________________________________________________________

From group  . . . . C##BDOC
To id . . . . . . . ________

OMVS gid  . . . . . ___________   (numeric id(suffix S for SHARED) or AUTO)

_  Copy permits only (target id may be a group or a user)
_  Generate RACF commands even when the target group exists
_  Copy CUSTOMDATA

Specify options for new group
/  Copy catalog aliases (only if CKFREEZE is present)
/  Issue ADDSD/RDEF for user resources
_  Copy RACFVARS profiles/members too (if option above selected)
```

Figure 37. GROUP COPY panel

The profile used as a model is shown at the top of the panel. In the **To id** field, specify the user or group to copy to. The **Generate RACF commands even when the target group exists** option forces the program to generate commands even when the user exists. A similar option is available on the User Copy panel.

When you copy a group, you can specify an OMVS GID to add an OMVS segment and assign the specified GID. When suffixed with an S (`1001S`, for example), the `SHARED` command keyword is added. You can also specify AUTO, which results in addition of the `AUTOGID` command keyword. The `SHARED` and `AUTOGID` command keywords are available in z/OS 1.4 or with APAR OW52135. On the User Copy panel, the option **Specify unique segment data** can be selected. This option opens a panel for specifying unique segment data. That is, the fields which normally are different for every segment type.

You must specify the **Copy permits only** option to permit copy operations from a group to a user or vice versa. The exact differences between a `COPY USER/GROUP` and a `COPY PERMIT` are detailed in "COPY" on page 740.

Use the options at the bottom of the panel to suppress the following actions:

- Cloning of catalog aliases.
- Cloning group-specific data set and general resource profiles along with catalog aliases.
- Only cloning of `RACFVARS` general resource profiles.

By default, the occurrence of a valid group ID as a member or key of a `RACFVARS` profile is considered meaningful, although RACF itself assigns no specific meaning to these occurrences.

For digital certificates some restrictions apply to the copying of profiles, due to the nature of the `RACDCERT` commands:

- Profiles in the `DIGTCERT` and `DIGTNMAP` classes cannot be copied directly.
- When copying a user profile with connected digital certificates, the latter cannot be copied.

To copy one or more model profiles, use option **RA.4 Mass update** - see "RA.4 MASS UPDATE - Specify mass copy/recreate/delete actions" on page 233.

CC - Copy to a different class

Use the **CC** line command for copying a general resource profile to a different class. It starts an equivalent to option **RA.4.3 Copy resource** for the profile it is

issued for.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Copy-Class
Command ===>

Copy general profile:
Class name  . . . . ACCTNUM
Profile pattern . . DUMMY

To class  . . . . . NEWCLASS
```

Figure 38. RESOURCE COPY-CLASS panel

To copy the profile, specify the class in the **To class**, then press **Enter**.

This command is only supported if zSecure Admin is installed and active.

CO - Add connect

Use the **CO** line command to add a connection to the group the command is issued for.

The panel it starts for a user is shown in Figure 39.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                     zSecure Suite - RACF - Add connect
Command ===> ____________________________________________________________

Create new connect
Userid  . . . . . . . . AUDIT     (user profile key)
Group . . . . . . . . . SYS*____  (group or filter)

Optional connect attributes
Authority . . . . . . . USE_____  (USE ,CREATE ,JOIN or CONNECT)
Default UACC  . . . . . NONE____  (N/R/U/C/A)
Connect owner . . . . . ________
Future revoke date  . . ________  (MM/DD/YY)
Future resume date  . . ________  (MM/DD/YY)
_  Revoke
_  Special          _  Operations       _  Auditor

Enter a group for a single connect.
Leave the field blank or enter a filter (e.g. SYS*) to get a selection list.
```

Figure 39. USER CONNECT panel

This command is only supported if zSecure Admin is installed and active.

When the CO command is issued for a GROUP, you can specify up to 10 IDs for connects.

When a group is entered in the group field, the connect command is generated. When the group field is left blank or a filter is used, a connect list is shown.

```
Add connects for userid AUDIT
 Command ===> _____________________________________________ Scroll===> CSR

Type CO in front of a group to add connect
   group    Complex   InstData
__ SYSAPPL  DINO      APPLICATION DATA
__ SYSAUTH  DINO      AUTHORIZATION GROUPS
__ SYSCTLG  DINO      CATALOG MANAGEMENT
****************************** Bottom of Data ******************************
```

Figure 40. Connecting via group filter

On this list, the **CO** action command generates a connect command with the parameters as specified in Figure 39 on page 57.

D or DD - Delete

Use the **D** line command to delete a profile and all references to it. The profile-related information that you can delete depends on the type of profile you are deleting.

- For users and groups, you can delete ID-specific profiles.
- For groups, you can also delete all related users when you delete the group profile.
- For DATASET profiles, you can also delete the covered data sets if you have specified a CKFREEZE data set as a data source. For more information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

You can also use the **DD** block line command to delete multiple profiles. Block commands must always be used in pairs. To mark the profiles, type a **DD** line command in the selection field for the first and last profile in the set of profiles to delete.

This command is only supported if zSecure Admin is installed and enabled.

When you run the **D** command for a group profile, the panel shown in Figure 41 is displayed.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Delete
Option  ===>

Group . . . . . . . C##BDOC

Specify action to perform
_  1. Delete group
   2. Remove group from resource profiles (remove permit)

Options for delete group                        Options for connected users
Enter "/" to select option(s)                   Delete all USERs ...
/  Dataset and id-specific profiles              _  owned by GROUP
   Only if previous is selected:                 _  connected to GROUP
   _  RACFVARS profiles and members              _  with defaultgrp GROUP
   /  Data sets and their catalog entries        Or move USERs to holding
   /  Incl. catalog entries without data sets           group ________
   /  Incl. uncataloged data sets

Change USERID in Notify fields to   ________  (default is NONOTIFY)
New Owner for non-dataset profiles  ________  (default is SYS1)
```

Figure 41. GROUP DELETE panel

The profile being deleted is shown at the top of the panel.

Select option **2** to only delete permits. To delete the group profile and all associated references, selection option **1**. When deleting a user profile, you can specify the following additional options for the delete action like moving the user to a holding group or only deleting occurrences in NOTIFY fields.

Dataset and id-specific profiles
Delete DATASET profiles and profiles where the ID occurs in a functional position. For more information, see "REMOVE" on page 870.

Options for connected users
Specifying users in a particular relation to the group that must be deleted or moved to a holding group.

Options for other id references
Specify replacement NOTIFY user IDs and owner IDs to replace those IDs that are deleted.

Any RACF and TSO commands created as a result of the query are sent to the CKRCMD file where you can review them. You can submit the commands from the CKRCMD file when you are ready.

For more information, refer to "RA.4 MASS UPDATE - Specify mass copy/recreate/delete actions" on page 233.

E - Event

Use the **E** line command to search for SMF events associated with the current or selected profile. You can issue this command on user, group, DATASET, and general resource profiles on profile displays.

This line command opens the Event panel for user, group, resource, or DATASET profiles depending on the profile type currently being viewed, which is equivalent to selecting the **EV.U**, **G**, **R**, or **D,** option from the Events menu. See "Interactive SMF processing for RACF" on page 550.

This command is only available if zSecure Audit is installed and active.

K - Manage APPCLU and PTKDATA keys

Use the **K** line command for changing, setting, or deleting the APPCLU session key or the PTKTDATA key value. This command is only permitted when the command is issued for an APPCLU SESSION segment or PTKTDATA SSIGNON segment.

When you run the **K** line command, the APPCLU session key panel opens, as shown in the following figure:

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                     zSecure Suite - APPCLU session key
Command ===> ____________________________________________________________

Class . . . . . . . . : APPCLU
Profile key . . . . . : NETWORK.LU001.LU002

Select the command you want to execute
_  1. Change or add session key ____________________  (hex x'hhhhhhhhhhhhhhhh'
      or character cccccccc)
   2. Delete session key
```

When option **1** (Change or add session key) is selected, you are required to specify the new session key. You can specify the key as a 1-8 character string or

a 1-16-digit hexadecimal number. Specify hexadecimal values as x'hhhhhhhhhhhhhhhh'. Use option **2** to delete the session key.

When you enter the **K** line command for the SSIGNON segment, the PTKTDATA key panel opens as shown in Figure 42.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - PTKTDATA key value
 Command ===> ____________________________________________________________

 Class . . . . . . . . : PTKTDATA
 Profile key . . . . . : MVSDINO.CRMRBYT

 Select the method you want to use to protect the key value
 1  1. Mask the key value using the masking algorithm
    2. Encrypt the key value (requires active cryptographic product)

 Key value . . . . . . . _________________  (16 hexadecimal characters)
```

Figure 42. PTKTDATA key value panel

From this panel, you can define the application key or a secured signon key and indicate the method for protecting the key value within the RACF database on the host. When defining the profile, you can either mask or encrypt the key. The key-value represents a 64-bit (8-byte) key that must be represented as 16 hexadecimal characters. The valid characters are *0-9* and *A-F*.

L - List

Use the **L** List line command for listing the current or selected profile. This command issues the appropriate RACF commands to list the profile. This behavior can be different depending on the profile class. It can be issued on any profile on profile displays.

The results of a listuser, listgrp, listdsd, rlist, or racdcert list command is presented in a browse panel.

To see the data sets covered by a DATASET profile, use either the **LD** (Listdsd DSNS) or the **LR** (List data sets covered via the Report line command).

LD - Listdsd DSNS

Use the **LD** (Listdsd DSNS) line command for listing the current or selected DATASET profile including the data sets covered by the profile. When this command runs, it issues a RACF listsdsd command with the DSNS keyword parameter.

Note: The **LD** line command only lists the data sets where the volume is online.

The results are shown in a browse panel.

LR - List data sets covered via Report

Use the **LR** (List via Report) line command for listing the data sets covered by the current or selected DATASET profile. When you run this command, it issues a recursive Security zSecure query.

Issuing a REPORT PROFILES type query has certain advantages over a RACF **LISTDSD DSNS** command apart from presentation. For more information, see "RA.3.1 Profiles - Profiles with their data sets" on page 196. Tape data sets on scratch tapes are not included in this standard query.

Also, CKGRACF permission is taken into account for the scope that determines what results you can see.

M - Move a user to another group

Use the **M** line command to move a user to a different department.

This command is only supported if zSecure Admin is installed and active.

The panel shown in Figure 43 opens when you run the M command.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Move
Option  ===>

Userid  . . . . . . C##BAHI

Move userid from or between groups

Group(s) from which user is to be moved:
________ ________ ________ ________ ________
________ ________ ________ ________ ________

Group(s) to which user is to be moved:
________ ________ ________ ________ ________
________ ________ ________ ________ ________
```

Figure 43. MOVE USER panel

The user you are moving is shown at the top.

You can specify one or more groups to remove the user from, and you can also specify one or more groups to connect the user to.

Connects are removed and created in accordance, and permits to group data set profiles of the old groups are removed as well.

MI - Manage information

Use the **MI** line command for viewing or modifying certain information contained in the profile it is issued for. The modify function is only available if the zSecure Admin product is active.

The panel it starts for a user is shown in Figure 44.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Information
 Command ===>

 Userid  . . . . . . USR0001

 Owner . . . . . . . C##B____
 Default group . . . C##B____
 Programmer name . . USER 0001________

 Installation data . TESTUSER FOR 2000-TEST, ESPECIALLY TO TEST THE    RACF DATA
BASE_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________

 Installation data   TESTUSER FOR 2000-TEST, ESPECIALLY TO TEST THE
 (as formatted by    RACF DATABASE
  RACF LISTUSER
  command output)
```

Figure 44. MANAGE USER INFORMATION panel

ML - Manage logon information

Use the **ML** line command for the following tasks:

- Revoke or resume a user either now or at a future date using a RACF function. To work with CKGRACF revoke/resume schedules, use the **MS** (CKGRACF Schedule) line command instead of this one.
- Change the password interval for a user ID.
- Set or delete the CKGRACF default password for a user ID.

The user you are working with is shown at the top. The installation data as formatted by the RACF `listuser` command is shown at the bottom.

The user information fields for User, DATASET, Group, and General resource profiles are listed in the following sections. You can modify the information in these fields. When you change the data, an appropriate command is generated.

User profile information fields
Table 19 list the information fields for user profiles.

Table 19. User profiles: User information fields

Field name	Description
Owner	The profile owner field
Default group	The user default group
Programmer name	The name associated with the user ID.
Installation data	The installation data

Group profile user information fields
Table 20 list the information fields for group profiles.

Table 20. Group profiles: User information fields

Field name	Description
Superior group	The `supgroup` field of the group
Owner	The profile owner field
Installation data	The installation data

DATASET profile user information fields
The only user information field for DATASET profiles is the **Installation data** field.

General resource profile user information fields
Table 21 list the information fields for group profiles. You can modify the information in these fields.

Table 21. General resource profiles: User information fields

Field	Description
Application data	The APPLDATA of the resource profile.
Installation data	The installation data.

This command is only supported if zSecure Admin is installed and active.

When you issue the **ML** line command, the panel shown in Figure 45 on page 63 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Manage logon-data
Command ===>

Userid  . . . . . . . : USR0001

Revoke date . . . . __________ (dd mmm yyyy, ddmmmyyyy, yyyy-mm-dd, or NOW)
Resume date . . . . __________ (dd mmm yyyy, ddmmmyyyy, yyyy-mm-dd, or NOW)

Password interval 30_   (NO or number)

Default password
_  1. Set password      ==>           ==>
   2. Delete password
```

Figure 45. LOGON DATA panel

The user you are working with is shown at the top.

To revoke or resume the user immediately, type *NOW* in the revoke date or resume date field. To perform the action at a later date, enter the date instead in one of the following date formats:

- *ddmmmyyyy*, 01jan2002 for example.
- *dd mmm yyyy*, 01 jan 2002 for example.
- *yyyy-mm-dd*, 2002-01-01 for example.

To set up a password that does not require the user to change it, specify *NO* for the password interval. To specify a password interval, enter the number of days up to a maximum of 254.

To set a CKGRACF default password, select **1 Default password**. Then, enter the password twice. To delete a CKGRACF default password, select **2 Delete**. Do not select a default password action if you want empty if you want To retain the CKGRACF default password, do not select a default password action.

If you set a CKGRACF default password for a user, it does not change the current password. To change the current password to this value, run the **P** (Password) line command.

MR - CKGRACF multiple authority requirement

Use the **MR** line command to show or change the CKGRACF multiple-authority requirement for a profile. This command can be issued on any profile in a profile display panel.

The CKGRACF multiple authority requirement specifies the number of administrators required to approve a CKGRACF command that targets the profile. This requirement only applies to commands that are subject to multiple authority. See “RA.2 QUEUED - Queued commands” on page 185.

This command is only supported if zSecure Admin is installed and active.

The **MR** line command starts the panel shown in Figure 46 on page 64.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Authority requirement
Command ===>

Class . . . . . : DATASET
Profile . . . . . : C##QAU3.**

List or set authority requirement for profile:
5  1. List
   2. Single
   3. Dual
   4. Triple
   5. Default
```

Figure 46. MULTIPLE AUTHORITY panel

The class and name of the profile you are now working with are shown at the top.

Use the **List or set authority requirement for profile** to specify the multiple authority setting for profiles.

In each case, a `CKGRACF AUTHORITY` command is generated.

```
  Menu  Utilities  Compilers  Help
------------------------------------------------------------------------------
 BROWSE    C##QAUS.C2R32AE.CKRTSPRT                  Line 00000000 Col 001 080
 Command ===>                                          Scroll ===> CSR
******************************** Top of Data ********************************
CKGRACF  AUTHORITY DATASET 'C##QAU3.**' LIST
CKG101I 00 Authority requirement for DATASET C##QAU3.** is DUAL
******************************** Bottom of Data *****************************
```

Figure 47. Multiple authority list result

MS - CKGRACF revoke/resume schedules

Use the **MS** line command to show or modify the revoke and resume schedules for a user.

This command is only supported if zSecure Admin is installed and enabled.

Revoke and resume schedules are the way that Security zSecure supports scheduling several revoked or resumed periods for a user. Refer to "Revoke/resume schedules" on page 1543 for an explanation.

This command is only supported if zSecure Admin is installed and enabled.

The **MS** line command starts the panel shown in Figure 48 on page 65.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - Manage User Schedules
 Option ===>

1  List           List schedules for this userid
2  Enable         Specify date(s) when user should be able to logon
3  Disable        Specify date(s) when user should not be able to log on
4  Wipe           Remove scheduled events at specified date(s)

 Userid  . . . . . . C##MBTJ2
 Schedule  . . . . . HOLIDAY_

 Start date  . . . . 13FEB1999_        End date  . . . . . 1999-02-22
                                       Number of days  . . ___

 Enter Reason below
'Well, he planned a holiday for when the tape would be ready... /A1'_____________
```

Figure 48. MANAGE SCHEDULE panel

The user ID you are working with is listed after the **Option** selection field. Table 22 describes the fields of interest.

Table 22. MANAGE SCHEDULE panel - field descriptions

Field	Description
Option	Specifies the action for the schedule. The following actions are available: • **1 List** shows the separate scheduled events for the user along with the overall schedule. • **2 Enable** or **3 Disable**, opens a panel for defining a time period during which the user can or cannot logon. Option • **4 Wipe** removes scheduled events from a period.
Schedule	Specifies the start date. Valid date formats are *ddmmmyyyy* and *1999-02-22*. You can also specify *TODAY*. This field is required for all actions except **1 List**.
Start date	The name of the schedule to change. This field is required for all actions except **1 List**.
End date	Specifies that the period to which the action applies extends up to and including this date. This field is optional and mutually exclusive with **Number of days**.
Number of days	The number of days the action is to last. This field is optional and mutually exclusive with **End date**.
Enter reason below	Optional specification of a reason for the action.

Each action results in a `CKGRACF` command. The result is typically shown in a browse panel.

```
COMMAND OUTPUT BROWSE ----------------------------- LINE 00000 Command failed
COMMAND ===>                                          SCROLL ===> CSR
******************************** Top of Data *********************************
CKGRACF USER C##BJT2 SCHEDULE HOLIDAY DISABLE (13FEB1999:1999-02-22) REQUEST   R
ould be ready... /A1")
CKG633I 08 Access to schedule 'HOLIDAY' denied for command in PARM string
CKG107I 08 Command ended with result code 8
CKG111I 08 Highest result code was 8
CKR962F Command failed, return code 8 (decimal)
******************************** Bottom of Data ******************************
```

Figure 49. Schedule disable result

In this case, the administrator issuing the command was not authorized to update the HOLIDAY schedule.

Figure 50 shows sample results from a LIST command.

```
CKGRACF LIST USER C##CX01 SCHEDULE
CKG132I 00 No CKGRACF queued command entries found
CKG116I 00 Scheduled revoke for HARD on 12Oct1999 by C##SYST 12Oct98 14:38
CKG116I 00 Scheduled resume for HOLIDAY on 01Mar1999 by C##DPT1  4Nov98 13:03
CKG116I 00 Scheduled resume for HOLIDAY on 10Mar1999 by C##DPT1  4Nov98 13:08
CKG116I 00 Scheduled resume for HARD on 12Aug2000 by C##SYST 12Oct98 14:38
Deleted  by C##SYST at 12 Oct 1998 14:39
CKG117I 00 --- Overall revoke/resume status ---
Resumed from  1 Mar 1999
Revoked from 12 Oct 1999
```

Figure 50. Schedule list result

After combining the separate schedules used, the overall revoke and resume status schedule, is shown in the lines preceding the `CKG117I` message. See Figure 50. The separate scheduled events are listed before the schedule it. In this example, no were specified. Message `CKG132I` indicates that no requests for scheduled events are queued for approval. See "RA.2 QUEUED - Queued commands" on page 185.

Because the **MS** line command is a command on the profile level, no scheduled event characteristics are passed. To work with a particular scheduled event, issue a line command for that event from the detail display.

The following line commands are available on a scheduled event:

D (Delete) generates an appropriate wipe command

C (Copy) reissues the command. Depending on your `SETUP CONFIRM` settings, you might have permission to change the command on the confirmation panel. If you do, you can use the panel as a template.

S (Select) shows the scheduled event in a more readable way, being split into items as must be specified on a request panel.

R (Repeat) opens a panel like the one shown in "RA.2 QUEUED - Queued commands" on page 185 with the characteristics of the event included so you can easily repeat it but without the `LIST` option.

I (Insert) opens the same panel without any data so you can add an event.

MT - Manage TSO information

Use the **MT** line command for the following tasks:

- Create a DATASET profile.
- Define a catalog alias in the master catalog.

- Create an ISPF profile data set for the current or selected user ID.

The **MT** command requires sufficient authorization for creating the specified profiles or catalog alias.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                         zSecure Suite - RACF - User Manage TSO
Command ===>

Userid for setup . : USR0001

Enter "/" to select option(s):
_  Create dataset profile for user
_  Define ALIAS in the Master Catalog
_  Create ISPF Profile Dataset
```

Figure 51. MANAGE TSO panel

Userid for setup
The user you are working with. This field is non-modifiable.

Create dataset profile for user
If this field is selected (with a /), an `ADDSD userid.** owner(userid)` command is generated, followed by a `SETROPTS REFRESH GENERIC(DATASET)`. Member `C2RSMUMH` in the `CKRPARM` configuration data set can be used to customize the generated commands.

Define ALIAS in the Master Catalog
If this field is selected, an `IDCAMS DEFINE ALIAS` command is generated. Member `C2RSMUMA`, located in the `CKRPARM` configuration data set must be customized to incorporate the User catalog name.

Create ISPF Profile Dataset
If this field is selected, a TSO ALLOC command is generated to create an ISPF profile data set. The data set name `userid.ISPPROF` can be changed by customizing member `C2RSMUMP` (located in the `CKRPARM` configuration data set).

MU - Manage installation-defined USRDATA

Use the **MU** line command for working with `USERDATA.` . It can be issued on any profile on profile displays.

For more information, see “RA.3.9 USERDATA - User data management” on page 219.

P - Change password and resume user

Use the **P** (Password) line command for managing password and password phrases and resuming user IDs. When you issue this command, the shown in Figure 52 on page 68 opens. The available actions are described in Table 23 on page 68. This command is only supported if zSecure Admin is installed and active.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                       zSecure Suite - RACF - User Password
 Command ===> ____________________________________________________________

 Userid  . . . . . . . : USR0001
 Name  . . . . . . . . : USER 0001
 Instdata  . . . . . . : TESTUSER FOR 2000-TEST, ESPECIALLY TO TEST THE    RACF DAT
 Last use date . . . . : 09Sep2009  Last use time . . . : 03:45
 Password changed  . . : 04Aug2009  Phrase changed  . . :
 Revoked . . . . . . . : No         Revoke inactive . . : No
 Revoke date . . . . . :            Resume date . . . . :
 Protected . . . . . . : No
 Select action:                                      Options
_  1. New password         ==>           ==>         /  Password expired
   2. DEFAULT password                               /  Resume userid
   3. PREVIOUS password                              _  Ignore pw history
   4. RANDOM password                                _  Bypass pw rules
   5. Resume only                                    _  Bypass pw exits
   6. Current password
   7. Make Protected
   8. New password phrase
```

Figure 52. PASSWORD panel

Table 23 describes the fields of interest on the RACF User password panel.

Table 23. RACF User password panel - field descriptions

Field	Description
Userid	Displays the currently selected user ID and the following related information: • User name. • Installation data. • Last date and time the user ID was used. • Date of the last password and password phrase change. • A flag indicating whether the user ID has been revoked. • If the user ID has been revoked and resumed, the revoke and resume dates are listed. • A flag indicating whether the user ID is protected. • Current® setting for the *Revoke inactive attribute* that indicates whether the user is effectively revoked due to the `SETROPTS INACTIVE()` setting.

Table 23. RACF User password panel - field descriptions (continued)

Field	Description
Select action	Specifies the action to perform when managing passwords and password phrases. You can select from the following actions. • **1 New password** Specify a new password. You must enter the new password twice. • **2 DEFAULT password** Set the password to the default password. • **3 PREVIOUS password** Set the user password back to its previous value. • **4 RANDOM password** Set the user password to some unknown value to ensure that the user ID cannot be used to logon. • **5 Resume only** Resume the user without changing the password. • **6 Current password** Resume the user ID and set the password to expired. • **7 Make Protected** Protect the user ID so that it does not have any password and cannot be used to logon. • **8 New password phrase** Add or remove a password phrase. Actions **2**, **3**, and **4** generate `CKGRACF` commands. Actions following actions **1**, **5**, **7**, and **8** generate either RACF or `CKGRACF` commands, depending on the `SETUP CONFIRM` settings.

Notes:

1. Setting a non-expired password might require more authorization than setting an expired one.
2. You can set the `CKGRACF` default password through the **ML** Manage Logon information line command.

`PE - Add or delete permit`

Use the **PE** line command for adding or deleting a permit for any profile type. This command is available for all profiles. This command is only supported if zSecure Admin is installed and active.

When you issue the **PE** command for a user or group, you can specify the DATASET or general resource profile for which you want to add or remove the permit. When issued for a DATASET or general resource profile, you can add permits for up to 10 users or groups. You can use a pseudo-access level `DELETE` to delete a permit.

Figure 53 on page 70 shows the panel that opens when you issue a **PE** command.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Add or delete permit
Command ===> ____________________________________________________________

Add or delete permit
Id  . . . . . . . . . . AUDIT     (user profile key)
Access level  . . . . . ________  (N/E/R/U/C/A/D)
Class . . . . . . . . . DATASET_  (class name or filter)
Profile key . . . . . . SYS1.*.**_____________________________________________
/  EGN mask
Profile type  . . . . . ______________________________

Optional conditions for the permit
When class  . . . . . . ________
When resource/profile
_______________________________________________________________________________
_____________________________________________________
```

Figure 53. USER PERMIT panel

If the **EGN mask** is not selected when you run the **PE** command, a permit command is generated. Otherwise, a panel opens with the PE selection list shown in Figure 54.

```
Add permits for id AUDIT                                        Line 1 of 4
Command ===> ____________________________________________________ Scroll===> CSR_
Type PE in front of an entry to Add permit      6 Dec 2006 00:07
   Class    Profile                                    Type    InstData
__ DATASET  SYS1.*.**                                  GENERIC
__ DATASET  SYS1.*.MAN*.**                             GENERIC
__ DATASET  SYS1.ACDS                                  GENERIC
__ DATASET  SYS1.BRODCAST                              GENERIC
****************************** Bottom of Data ********************************
```

Figure 54. Adding permits using a mask

If you select a DATASET or general resource profile, you can specify up to 10 user IDs.

On this list, the PE action command generates a Permit command with the parameters as specified on the previous panel.

R or RR- Recreate a profile

Use the **R** line command on any profile in a profile display to generate the commands to recreate the profile. For user and groups, you can also recreate the associated access list entries and DATASET and resource profiles. It can also be used to recreate segments by issuing the command on a segment display.

This command is only supported if zSecure Admin is installed and active.

Use this command for restoring a profile that was inadvertently deleted from the database:

1. Restore a version of the database in which the profile still existed to a data set. Then, use it as a COPY.TEMP input data source. See "SE SETUP - Options and input data sets used" on page 1641.
2. Locate the profile of interest in the view of the restored database.
3. Run the **R** line command on the profile.

Note: Using an UNLOAD data set as an input source has the disadvantage that passwords and other sensitive fields are recreated as .********.

You can also use the **R** line command to create a copy of a profile. After running the command, edit the generated commands to create a copy of the profile instead of recreating the same profile.

To recreate multiple profiles at one time, use the block line command **RR**. Block commands must always be used in pairs. To mark the profiles, type an **RR** line command in the selection field for the first and last profile in the set of profiles to recreate.

The **R** line command has the following limitations:

- General Resource profiles in the following classes cannot be recreated using this mechanism: DCEUUIDS, DIGTCERT, DIGTNMAP, DIGTRING, IDIDMAP, UNIXMAP, NDSLINK, NOTELINK, ROLE.
- Certificate, ring, and map connections on a user ID cannot be recreated.
- TAPEDSN profiles cannot be recreated.
- Multivolume discrete data set profiles might be handled incorrectly.
- Discrete profile ADDSD only works if the data set is cataloged, and you might have to add NOSET and VOLUME to the commands.
- Last change time stamps reflect the time the profile was recreated.
- Connect owners are not preserved because RACF commands do not permit arbitrary owners to be specified. Connect owners are not used for RACF authorization decisions.

When you issue the **R** line command for a user, the panel shown in Figure 55 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                       zSecure Suite - RACF - User Recreate
Command ===> ____________________________________________________

Recreate userid . . USR0001

Specify options for recreate
/  Copy Dataset and General Resource profiles for this user
/  Copy Access List entries with this user
/  Use CKGRACF to update the user profile
```

Figure 55. USER RECREATE panel

The profile you are recreating is shown at the top.

You can specify whether the commands generated to update the profile can include CKGRACF commands. For a user or group, you can opt to restore access list entries and associated DATASET and general resource profiles as well.

Figure 56 on page 72 shows a sample of the results of a RECREATE command operation.

```
BROWSE - MYTSOID.C2R1EF2A.CKRCMD ------------------- LINE 00000000 COL 001 080
COMMAND ===> _____________________________________________ SCROLL ===> CSR
******************************** Top of Data ********************************
       /* CKRCMD file CKR1CMD complex DINO NJE <LOCAL> generated  2 Feb 1999 16
       /* CKRCMD file CKR1CMD complex DINO NJE <LOCAL> generated  2 Feb 1999 16
       adduser USR0001  owner(C##B) dfltgrp(C##B)
       altuser USR0001  name('USER 0001           ')
       password user(USR0001 ) interval(30)
       connect USR0001  group(C##B    ) owner(C##B    )  auth(USE) uacc(NONE)
       altuser USR0001  tso(msgclass(A))
       altuser USR0001  tso(proc(TSOPROC2))
       altuser USR0001  tso(size(9000))
       altuser USR0001  tso(maxsize(16000))

       ckgracf field USER     USR0001  set password('E40B16EBE88BD808'X)
       addsd  'USR0001.**' GENERIC   owner(USR0001) uacc(NONE   ) audit(failure
       permit  'USR0001.**' GENERIC id(C##B) access(READ)
       permit  'USR0001.**' GENERIC id(C##AINT) access(ALTER)
       permit  'USR0001.**' GENERIC id(C##BAH2) access(ALTER)
       permit  'USR0001.**' GENERIC id(C##BHOF) access(UPDATE)
       permit  'USR0001.**' GENERIC id(C##BHO2) access(UPDATE)
       permit 'C##A.L.**' GENERIC id(USR0001) access(READ)
       permit 'C##BAH2.**' GENERIC id(USR0001) access(ALTER)
       permit 'C##CCW1.**' GENERIC id(USR0001) access(ALTER)
       permit 'C##CCW2.**' GENERIC id(USR0001) access(ALTER)
```

Figure 56. Recreate results

For more information, see "RA.4 MASS UPDATE - Specify mass copy/recreate/delete actions" on page 233.

S - Select

The **S** line command is available on all profiles, provided additional information was requested in your query. Issuing this line command opens an ISPF panel that shows more detailed information about the profile.

SE - Show application segments

Use the **SE** (Segments) line command for generating a recursive query to view the application segments for the current or selected profile. It can be issued on any profile on profile displays.

The advantage of using **SE** to retrieve application segments on a per profile basis instead of specifying that they are always to be included immediately (by tagging **Show segments** and **All** on a profile selection panel) is to limit the required amount of storage. With SE command processing, the program does not have to store all the application segments for the other profiles.

Figure 57 shows the panel that opens when you run the **SE** line command.

```
zSecure Admin Display Selection                  1 s elapsed, 0.3 s CPU
 Command ===>                                                Scroll===> CSR

   Name     Summary Records Title
 _ CICS           1       1 zSecure Admin USER C##BMR1 CICS segments
 _ NETVIEW        1       1 zSecure Admin USER C##BMR1 NETVIEW segments
 _ OMVS           1       1 zSecure Admin USER C##BMR1 OMVS segments
 _ TSO            1       1 zSecure Admin USER C##BMR1 TSO segments
 ****************************** BOTTOM OF DATA ******************************
```

Figure 57. USER SEGMENTS panel

The segments shown depend on the ENTITY type. Figure 57 shows the panel for USER profiles.

When you select a segment that interests you, a panel like the one shown in Figure 58 opens.

```
zSecure Admin USER CRMBMR1 OMVS segments                      Line 1 of 1
Command ===> ____________________________________________ Scroll===> CSR_
                                          8 Aug 2006 10:23
   User     Complex  Uid         Home directory                  Initial progr
__ C##BMR1  DINO     __________0 /u/c##bmr1_____________________ /bin/sh______
****************************** Bottom of Data ********************************
```

Figure 58. USER SEGMENT overview panel

The Application segment display panel usually shows the profile name and the complex name on the left side of the display. The other fields shown depend on the current segment shown in the panel, as detailed in the field descriptions.

SR - Show all Relevant information

Use the **SR** line command for showing all information related to a user or group. The resulting display panels include the user or group profile, all profiles with the user or group in their name or member list, and optionally all profiles with the user or group on the access list, and all profiles within the scope of the user or group.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Show all details
Command ===>

Show structured information for userid:

Userid  . . . . . . . : C##BGU3

Include profiles in display where userid is:
/  On access list
/  Within scope            (only for central administrators)
/  Application segments     (only for central administrators)
/  Digital certificates     (only for central administrators)
```

Figure 59. USER SHOW ALL panel

The user or group you are working with is shown at the top.

The following output options are available for the detail results.

Table 24. Output options for User or Group information display

Field	Description
On access list	Include all profiles with the user or group on the access list. This list does not include profiles that have indirect access through a group on the access list.
Within scope	Include all profiles within the scope of the user or group. This option is not permitted in restricted mode.
Application segments	Include all application segments. This option also selects `STARTED` `STDATA` segments with a started user or group equal to the user or group ID, and `DATASET` `DFP` segments with a resource owner equal to the user or group ID. This option is ineffective in restricted mode.
Digital certificates	Include all certificates and key rings associated with this user. This option is ineffective in restricted mode

A sample overview display is shown in Figure 60.

```
zSecure Admin Display Selection                    2 s elapsed, 1.2 s CPU
Command ===>                                                Scroll===> CSR

  Name     Summary Records Title
_ USER           1       1 zSecure Admin USER C##BGU3 basic information
_ OMVS           1       1 zSecure Admin USER C##BGU3 OMVS segments
_ OPERPARM       1       1 zSecure Admin USER C##BGU3 OPERPARM segments
_ TSO            1       1 zSecure Admin USER C##BGU3 TSO segments
_ WORKATTR       1       1 zSecure Admin USER C##BGU3 WORKATTR segments
_ DIGTRING       0      24 zSecure Admin USER C##BGU3 Key rings
_ PROFILES       1       1 zSecure Admin profiles with C##BGU3 in key or m
_ OWNER          1       1 zSecure Admin profiles owned by C##BGU3
_ ACCESS         1       1 zSecure Admin profiles with C##BGU3 on access l
_ SCOPE        409    2434 zSecure Admin profiles in scope of USER C##BGU
****************************** BOTTOM OF DATA ******************************
```

Figure 60. All relevant user information

TR - Trust bestowed on userid

Use the **TR** action command for running a TRUSTED report for the current or selected user. This command is only supported if zSecure Audit is installed and configured.

For additional information, see "TRUSTUSR - Trusted users report" on page 292.

X or XX- Exclude a profile from FORALL processing

Use the **X** line command to exclude a profile from FORALL processing. To exclude multiple profiles, type **X** in the selection field for each profile to exclude. You can also use the **XX** block command to exclude a block of profiles. This line command must be used in pairs. To mark the profiles, type the **XX** line command in the selection field for the first and last profile in the set of profiles to be excluded.

You cannot combine the Exclude (**X** or **XX**) line command with the Select line command (**Z** or **ZZ**).For more information, see the "FORALL command" on page 13.

Z or ZZ - Select a profile from FORALL processing

Use the **Z** line command to select a profile for FORALL processing. To select multiple profiles, type **Z** in the selection field for each profile to select. You can also use the block command to mark the beginning and end of the set of profiles to be selected. You cannot combine the Include line command (**Z**, **ZZ**) with the Exclude (**X**, **XX**) line commands. For more information, see the "FORALL command" on page 13.

34 - Data set list utility

This action command invokes program ISRUDL, which can also be called using IBM ISPF option 3.4. The action command is available on user, group, and DATASET profile overviews. When this command is run, a data set list panel is displayed with the profile in the dsname level.

Line commands on detail displays

The line commands available on detail displays depend on the type of field that is shown. Most fields support the following standard line commands listed in Table 25 on page 75.

Table 25. Standard line commands available on detail displays

Line command	Meaning
C	Copy the field or entry. For example, issuing the **C** command for an access list entry creates a `PERMIT` command to add a new access list entry with the same permissions. Before the command is run or queued, you are prompted with a panel to edit the key or profile name.
D	Delete the field or entry. For example, issuing the **D** command before a volume serial generates an `ALTDSD DELVOL` command.
L	Use the **`LIST`** line command to list the information for the currently selected entry. For example, issuing an L command before a NOTIFY field generates a `LISTUSER` command.

Note: If your installation is configured to queue generated commands before running them, you view and manage any commands generated by a line command through the **RA.2 Queued commands** option. See "RA.2 QUEUED - Queued commands" on page 185.

Some detail views support additional line commands. For more information, see the following topics.

- "Access List detail view"
- "Connect detail view" on page 77
- "Data set detail view" on page 78
- "Digital Certificate detail view" on page 78
- "USR fields" on page 78
- "RACLINK fields" on page 79

Access List detail view: On access list display panels, the following commands are supported: **L** List, **C** Copy, and **D** Delete, **L** issues a RACF `listuser` or `listgrp` command (as appropriate) and shows the results in a browse panel. You can use the **C** and **D** commands for adding and deleting permits. Figure 61 on page 76 shows a sample of the results.

```
zSecure Admin General resource overview                          Line 1 of 77
 Command ===> _____________________________________________ Scroll===> CSR_
 Class PROGRAM                              29 Mar 2006 15:04


 _ Identification                                                      FETP
   Class                        PROGRAM
   Profile name                 CNRACF
   Type
   Volume serial list
 _ Owner                        C##AINT_ ZSECUR GROUP ADMIN
   Installation data            ________________________________________________
   Application data             ________________________________________________

   User     Access  ACL id   When              Name                  InstData
 c -group-  READ___ C##A____ ________ __________                      C## MANAG
 _ -group-  READ___ C##ARACF ________ __________                      DIRECT LI
 _ -group-  READ___ C##B____ ________ __________                      C## WERKN
 _ -group-  READ___ C##BRACF ________ __________                      DIRECT LI
 _ -group-  READ___ C##C____ ________ __________                      EXTERNE G
 _ -group-  READ___ C##CDEMO ________ __________                      FOR CONSU
 _ -group-  READ___ C##CXGRP ________ __________                      GROUP TO
 _ -group-  READ___ C##GRACF ________ __________                      PADS LIVE
 _ -group-  READ___ C##QA___ ________ __________
 _ -group-  READ___ SYSAPPL_ ________ __________                      APPLICATI
 _ -group-  ALTER__ SYSPROG_ ________ __________                      SYSTEM PR
 _ C##AINT  ALTER__ C##AINT_ ________ __________ ZSECUR GROUP ADMIN
 _ C##ASCH  ALTER__ C##ASCH_ ________ __________ SCOTT HENDRIX

   Members
 _ ZSECUR.CNRNEW.CNRLOAD//PADCHK_____________________________________________
 _ ZSECUR.CNR250S.PR00216.CNRLOAD//PADCHK_____________________________________
 _ ZSECUR.CNRNEW.SC2RLOAD//PADCHK_____________________________________________
 _ ZSECUR.C2R110.RC2R110.SC2RLOAD//PADCHK_____________________________________
```

Figure 61. RESOURCE DETAILS panel

The **C** line command opens a panel to copy the permit as shown in Figure 62.

```
   Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Copy permit
Command ===> ____________________________________________________________________

Change at least one field
User or group  . . . C##A____          (was group C##A)
Access level . . . . READ___           (was READ)
Class  . . . . . . . PROGRAM_          (was PROGRAM)
Profile name . . . . CNRACF_____________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_____________________________________ (was CNRACF)



Optional conditions for the permit
When class . . . . . ________           (was empty)
When resource/profile
_______________________________________________________________________________
_____________________________________________________________(was empty)
```

Figure 62. COPY PERMIT panel

Pressing ENTER generates a command to create a copy of the permit, and presents it in a confirmation panel. The options shown on this panel depend on your SETUP CONFIRM settings. An example is shown in Figure 63 on page 77.

```
                        zSecure Suite - Confirm command
Command ===> ____________________________________________________________

Confirm or edit the following command
permit_CNRACF_class(PROGRAM)_id(C##A)_access(READ)_____________________
_______________________________________________________________________
_______________________________________________________________________


Command execution . 4  1. QUEUE RACF command
                       2. QUEUE CKGRACF command (allows use of Reason)
                       3. ASK administrator to execute CKGRACF command
                       4. REQUEST CKGRACF command for later execution
                       5. WITHDRAW CKGRACF command

Specify date for command to be executed
Start date . . . . .  __________  (ddmmmyyyy, yyyy-mm-dd or TODAY)
Until/for  . . . . .  __________  (ddmmmyyyy, yyyy-mm-dd or number of days)
Reason . . . . . .    ____________________________________________________

Press ENTER to continue or END to cancel the command
```

Figure 63. CONFIRM PERMIT panel

At the top, the command to be generated is shown. The **D** command results in a similar panel.

Connect detail view: On connect displays, **L** List, **C** Copy, and **D** Delete are supported. **L** issues a RACF `listusr` or `listgrp` command as appropriate and shows the results in a browse panel. You can also use the **C** and **D** commands for adding and removing connects. Figure 64 shows an example of the Group detail panel.

```
zSecure Admin GROUP C##A Overview                          Line 1 of 46
Command ===> ____________________________________________ Scroll===> CSR
like C##A                                    20 Sep 2000 00:50


_ Identification                                                    ETPS
_ RACF group name              C##A
_ Superior group               C#_____
_ Owner                        C#_____
  Installation data            MANAGEMENT_____________________________

  User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt    Name
c C##AINT_ CREATE_ _ S__ __ NONE___ ___________ ___________ GROUP ADMINISTRAT
_ C##BGUS_ USE____ _ S__ __ NONE___ ___________ ___________ GUS BAINES
_ C##ASCH_ CREATE_ _ ___ __ NONE___ ___________ ___________ S HENDRIX
_ C##ATST_ USE____ _ ___ __ NONE___ ___________ ___________
_ C##CX01_ USE____ _ ___ __ NONE___ ___________ ___________ TEST USER, NO TSO
_ C##BPK2_ USE____ R ___  G NONE___ ___________ ___________ PETE KENDALL

  SubGroup InstData
_ C##AAPPC APPC DEVELOPMENT
_ C##ARACF DIRECT LIVE RACF+SMF
_ C##BRACF DIRECT LIVE RACF+SMF+PADS
_ C##DELET

  Safeguards                          Statistics
  Terminal use authorization   No_    Creation date                4Nov95
  Universal access authority   NONE
  Data set model profile name  ____________________________________________
```

Figure 64. GROUP details panel

The **C** line command opens the Copy Connect panel shown in Figure 65 on page 78.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - RACF - Copy connect
Command ===> ____________________________________________________________

Create connect like existing connect of group C##A
Change at least one field
Userid . . . . . . . C##AINT_ (was C##AINT)
Group  . . . . . . . C##A____ (was C##A)

Optional connect attributes
Authority  . . . . . CREATE_
Default UACC . . . . NONE____
Connect owner  . . . ________
Future revoke date . __________ (YYYY-MM-DD or DD MMM YYYY)
Future resume date . __________ (YYYY-MM-DD or DD MMM YYYY)

_  Revoke
/  Special  _  Operations  _  Auditor

Optional processing mode
_  Modify existing connect
```

Figure 65. COPY CONNECT panel

Data set detail view: When you are in a detail display showing a data set (fields **DSN**, **DATASET**, or **DSNAME)**, you can specify the **B** line command to browse the data set.

Digital Certificate detail view: Certificates are shown for both the USER BASE segment and the DIGTRING CERTDATA segment and are processed slightly differently in each location.

For the USER BASE segment, the certificates created for this user are shown with both **label** and **name**. The following actions commands are supported for both of these fields:

L list generates a RACDCERT LIST command, which is directly run by RACF.

D delete generates a RACDCERT DELETE command, which is presented in a panel like the one for the ACL D (Delete) command.

C copy generates a RACDCERT CONNECT command.

On the DIGTRING CERTDATA segment, the certificates connected to this ring are shown. The following action commands are supported for this segment.

L list and **D** Delete are the same as they are for the

D delete generates a RACDCERT REMOVE command, which is presented in a panel like the one for the ACL DELETE command.

C copy generates a RACDCERT CONNECT command.

These generated commands are shown on a panel where they can be edited if necessary.

USR fields: The USR fields are used for two, mostly separate functions within Security zSecure: *normal* user-defined fields and CKGRACF fields. Different line commands are available for each USR field type. You can view and manage normal user-defined fields through option **RA.3.9 USERDATA**. See "RA.3.9 USERDATA - User data management" on page 219. Table 26 on page 79 describes the line commands available on the detail display for normal, user-defined fields.

Table 26. Normal, user-defined USR fields: available line commands

Line command	Description
C	Copy the USERDATA entry, prompting you for new parameters. The copied entry has the Entry Name, Flag, and Value set as in the repeated entry.
D	Generates a CKGRACF DELETE command.
I	Add a USERDATA field to a specified profile.
R	Generates a CKGRACF REQUEST command with a copy of the current command. You can edit the command before running it.
S	SET. This command takes you to a panel where the current USERDATA field is described completely. You can edit this panel to reflect the changes that you want to make to this field.

You can view and manage the CKGRACF fields through option **RA.2. Queued commands**. See "RA.2 QUEUED - Queued commands" on page 185. Table 27 describes the line commands available on the detail display for CKGRACF USR fields.

Table 27. CKGRACF USR fields: available line commands

Line command	Description
A	Approve the queued command.
C	Copy the USERDATA entry, prompting you for new parameters. The copied entry has the Entry Name, Flag, and Value set as in the repeated entry.
D	Deny the queued command.
H	Generates a CKGRACF HOLD command for the command in the approval queue. Running this command refreshes the last action time stamp of the command, which defers expiration.
I	Specify another command to add to the queue of approved commands.
R	Edit the current command and queue for approval.
S	View the details of the selected command.

RACLINK fields: On User profile detail display panels, you can manage RACLINK associations for a user from the *Linked.node.user* fields available from the User Profile detail view. If the current user has a RACLINK association defined, the information is listed in the *Linked.node.user* field as shown in Figure 66 on page 80. If no RACLINK association is defined, the RACLINK entry fields are empty. However, you can add an association by typing the **I** (Insert) line command in the input field for the *Linked.node.user* entry field.

```
zSecure Suite USER IBMUSER overview
Command ===> _____________________________________________ Scroll===> PAGE
Users like IBMUSER                          10 Sep 2010 23:36

  Log all user actions   UAUDIT No
  Linked node.user  Type   Stat Pwd  Defined (GMT)    Approved (GMT)   Creator
_/ CRM4.CRMAJEN     Peer         ____ 1997/04/09 17:14 1997/04/09 17:14 CRMAJEN
  Digital certificate labels      Digital certificate names

  ____________________________
  Certificate filter label

  ____________________________
```

Figure 66. RACLINK associations for a user

In Figure 66, IBMUSER has a RACLINK association with the user profile CRMAJEN. Authorized users can modify the values for the *Linked node.user*, *Type*, and Pwd fields by typing over the existing values in these fields. Table 28 lists the line commands available to manage RACLINK associations for the user profile.

Table 28. RACKLINK fields: available line commands

Line command	Description
A	Approve a pending association. This command is only supported for association records having *Pend* status. If the command is issued on an association that is not pending, an error message is displayed.
C	Copy the current RACLINK association. When you run this command, the Copy RACLINK panel opens to complete the copy operation. Press F1 on this panel for help.
D	Generates a RACLINK id (userid) undefine (linked.node.user) command to delete the current RACLINK association. Depending on your Setup Confirmation options (SE.4), when you run this command, it either deletes the association immediately or opens a confirmation panel to set command processing options for deleting the association.
I	Copy or insert a RACLINK association for the current user. When you run this command, the Copy/Insert RACLINK panel opens to specify the information for the association. Press F1 on this panel for help.

Line commands on non-profile displays

Additional line commands are available on certain non-profile displays. These commands are described in the documentation for these panels, "Line commands on the class settings display" on page 176 for example.

Line command status messages

After you specify a line command on an overview or detail display panel and press **Enter**, the corresponding command is generated. A status message is also shown in the upper right corner of the panel to indicate the status of the action. Table 29 provides examples of line command status messages.

Table 29. Line command status messages

Message	Meaning
Successfully modified **Copy successful** **Delete successful**	Indicates that a RACF command was generated and run. The command action must be set to EXECUTE.

Table 29. Line command status messages (continued)

Message	Meaning
Queued in CKRCMD	Indicates that a RACF command was generated and either written to the CKRCMD file for later execution or for submission to another MVS system. The command action must be QUEUE.
Queued in CKR2PASS	Shows that a Security zSecure command was generated and written into the CKR2PASS file. You must run Security zSecure again with these commands as input to generate RACF commands. This message is issued when a user or group profile is copied or deleted. The command action can be either QUEUE or EXECUTE.
Refresh registered	Indicates that a RACF SETROPTS REFRESH command was generated. The command has not been run yet. When you leave the results panel, another panel opens for confirming all generated SETROPTS REFRESH commands. Only the confirmed commands are run. The command action must be set to EXECUTE.

Managing the Access List display panel

When working with profiles in zSecure, you can view and manage the access list for profiles from the profile display panels. You can use the access list information to research access levels and determine how profile changes affect the access list.

You can specify the default format for the access list from on the Setup - View panel available on the SETUP menu. You can also control the format using the ACL primary command from the command line.

Table 30 lists the format options available on the Setup-View panel.

Table 30. Access list format field values

Value	Description
No	Do not show the access list.
Sort	Sort the entries in the access list view by **Id**, **User**, or Access, as specified under the Access list sort column.
Explode	Replaces groups on the access list by the users granted access through the group profile definition and connect attributes. Also adds administrative access. This format is useful for determining the effects of removing a group ID.
Resolve	This format is like the **Explode** option, but shows the resolved access per user: superfluous entries are removed.
Effective	Extends the **Resolve** result by adding users with OPERATIONS or group-OPERATIONS attributes.

If the Access list format field on the Setup - View panel is set to a value other than NO, you can use the ACL primary command to control the data shown on an Access list display panel. Table 31 on page 82 lists the ACL command parameters you can specify.

Table 31. Access list display: ACL primary command parameters

Parameter	Description
EXPLODE	All lines containing a group are replaced by lines for all users connected to the group. Operations access is also shown if the relevant profiles were read, which can be requested through the **Enable full ACL** option. Also shows access permitted by the owner field, group-special, group-operations, connect CREATE authority, class authorization, system operations, or a qualifier.
RESOLVE	Includes 1 line per user or user plus `WHEN(class(profile)` condition, showing actual access. Does not show access permitted by operations, group-operations, or administrative access.
EFFECTIVE	Creates a view like the RESOLVE view but also shows access due to system-wide or group operations. This command requires a full database read using the **Enable full ACL** option. The command fails if a query is run with an indexed read.
NORMAL or **ASIS**	Only show access list entries without exploding or resolving the data.
TRUST	Creates a view like the `EXPLODE` view but provides separate entries for administrative and normal data access.
SCOPE and **NOSCOPE**	Determines whether administrative access is shown in the access list data. This setting is automatically switched to `NOSCOPE` for the following views: `NORMAL`, `RESOLVE`, and `EFFECTIVE`. The setting is automatically switched to `SCOPE` for the `EXPLODE` and `TRUST` views. To change the default setting, you can specify the option behind the ACL primary command, **ACL EXPLODE NOSCOPE** for example.
UNIVERSAL and **NOUNIVERSAL**	Determines whether default connections to universal groups and system-wide operations are used to calculate access.
SORT	Changes the sequence of the data display. See Table 32.

To change the sequence of a display, you can specify the SORT option on the Setup - View panel, or use the SORT parameter with the ACL primary command.Table 32 lists the SORT parameter options.

Table 32. Access list display: ACL command SORT parameter options

Parameter	Description
ID	Sort by ID actually in access list. This option is available for user or group profiles.
USER	Sort by user ID. The user ID can be present in the exploded access list data for a group.
ACCESS	Sort by access level, from high access to low access.

In Figure 67 on page 83 a normal sorted ACL is shown, sorted by User.

```
zSecure Admin DATASET overview                                Line 1 of 35
Command ===> _____________________________________________ Scroll===> CSR_
All profiles                                  9 Feb 1999 00:05

  Identification                                                      DINO
  Profile name                 R##PROB.P.**
  Type                         GENERIC
  Volume serial list
_ Effective first qualifier    R##PROB  ROB VAN HOUTEN
_ Owner                        R##PROB_ ROB VAN HOUTEN
  Installation data            ____________________________________________

  User     Access  ACL id   When               RI Name        DfltGrp    RvC
_ -group-  READ___ C##A     ________ __________                C##HOLD    No
_ -group-  READ___ C##B     ________ __________                C##HOLD    No
_ C##BERT  READ___ C##BERT  ________ __________ RI BERT LANG
_ R##PROB  ALTER__ R##PROB  ________ __________ RI ROB HOUT

  Safeguards                          Other permissions
  Erase on scratch             No_    Allow all accesses    WARNING No_
  Audit access success/failures __R   Universal access authority    NONE___
  Global audit success/failures ___   Resource level                _0
_ User to notify of violation  R##PROB_
  Days protection provided #   _____

  Mandatory Access Control            Statistics
  Security label               ________ Creating user's connect group C##B
  Security level                       Creation date                 14Nov95
  Categories list
******************************* BOTTOM OF DATA ********************************
```

Figure 67. ACL Display - SORT USER

In the standard format, the groups are listed at the top of the panel, showing `-group-` in the User column. The user IDs explicitly on the ACL are sorted and shown under the groups. Issuing the `ACL SORT ACCESS` command opens the panel shown in Figure 68 on page 84.

```
zSecure Admin DATASET overview                                  Line 1 of 35
Command ===> ____________________________________________________ Scroll===> CSR_
All profiles                                    9 Feb 1999 00:05

  Identification                                                        DINO
  Profile name                  R##PROB.P.**
  Type                          GENERIC
  Volume serial list
_ Effective first qualifier     R##PROB  ROB HOUT
_ Owner                         R##PROB_ ROB HOUT
  Installation data             ____________________________________________

  User     Access  ACL id   When               RI  Name        DfltGrp      RvC
_ R##PROB  ALTER__ R##PROB  ________ __________ RI ROB HOUT
_ -group-  READ___ C##A     ________ __________                C## MANAGE   No
_ -group-  READ___ C##B     ________ __________                C## WERKNE   No
_ C##BERT  READ___ C##BERT  ________ __________ RI BERT LANG

  Safeguards                          Other permissions
  Erase on scratch              No_   Allow all accesses    WARNING No_
  Audit access success/failures __R   Universal access authority    NONE___
  Global audit success/failures ___   Resource level                _0
_ User to notify of violation   R##PROB_
  Days protection provided #    _____

  Mandatory Access Control            Statistics
  Security label                ____  Creating user's connect group C##B
  Security level                      Creation date                 14Nov95
  Categories list
******************************* BOTTOM OF DATA ********************************
```

Figure 68. ACL Display - SORT ACCESS

Changing the format to **ACL EXPLODE** and **ACL UNIVERSAL**, results in the view shown in Figure 69.

```
zSecure Admin DATASET overview                                  Line 1 of 126
Command ===> ____________________________________________________ Scroll===> CSR_
All profiles                                    9 Feb 1999 00:05

  Identification                                                        DINO
  Profile name                  R##PROB.P.**
  Type                          GENERIC
  Volume serial list
_ Effective first qualifier     R##PROB  ROB HOUT
_ Owner                         R##PROB_ ROB HOUT
  Installation data             ____________________________________________

  User     Access  ACL id   When               RI Name          DfltGrp    RvC
_ C##AINT  OWNER   C##A     ________ __________ GROUP ADMIN
_ R##PROB  OWNER   R##PROB  ________ __________ ROB HOUT          C##HOLD   No
_ R##PROB  QUALOWN R##PROB  ________ __________ ROB HOUT          C##HOLD   No
_ C##BMR1_ ALTER-O - oper - ________ __________ MARK ROSE
_ C##QAN24 ALTER-O - oper - ________ __________ REVOKED FOR QR71113
_ IBMUSER_ ALTER-O - oper - ________ __________ IBM DEFAULT USER
_ R##SLIN_ ALTER-O - oper - ________ __________ BERT LANG
_ R##PROB  ALTER__ R##PROB  ________ __________ ROB HOUT
_ CERT001_ READ___ C##B____ ________ __________ TESTUSER DIG.CERT
```

Figure 69. ACL Display - EXPLODE

The EXPLODE format shows OPERATIONS just like the EFFECTIVE format. The access reported is ALTER-O, which is considered to be higher than ALTER (for the previous SORT order is still active). The user IDs reported with the OPERATIONS attribute are all system-wide OPERATIONS users. For groups with the OPERATIONS attribute, the group is reported under **ACL id** instead of - *oper* -.

A fair number of the users selected might have access through both groups, so after switching to **ACL EFFECTIVE**, some superfluous entries (where the determination of effective access is concerned) are deleted. As a result, the line count goes down.

```
zSecure Admin DATASET overview                          Line 1 of 113
Command ===> ____________________________________________ Scroll===> CSR_
All profiles                                  9 Feb 1999 00:05

  Identification                                                  DINO
  Profile name                R##PROB.P.**
  Type                        GENERIC
  Volume serial list
_ Effective first qualifier   R##PROB  ROB VAN HOUTEN
_ Owner                       R##PROB_ ROB VAN HOUTEN
  Installation data           ________________________________________

  User     Access  ACL id   When                RI Name                 DfltGrp   RvC
_ C##QAN24 ALTER-O - oper - ________ __________   REVOKED FOR QR71113
_ IBMUSER_ ALTER-O - oper - ________ __________   IBM DEFAULT USER
_ R##SLIN_ ALTER-O - oper - ________ __________   BERT LANG              C##HOLD  No
_ R##PROB  ALTER__ R##PROB  ________ __________   ROB HOUT               C##HOLD  No
_ CERT001_ READ___ C##B____ ________ __________   TESTUSER DIG.CERT
_ CERT002_ READ___ C##B____ ________ __________   TESTUSER DIG.CERT
```

Figure 70. ACL Display - EFFECTIVE

In Figure 70, the operations access lines have disappeared because the user ID *C##BMR1* has explicit access through group *C##B*. As a result, the OPERATIONS attribute is effectively ignored.

When ACL RESOLVE is requested now, the first three entries disappear.

Table 33 lists the fields available to show the access list information:

Table 33. Access List: display fields

Field name	Description
User	ID on access list.
Access	Access level.
ACL id	ID mentioned on access list.
When	Condition for this access to be granted.
RI	The user status (inactive, revoked, or pending). This field indicates whether the user would be revoked due to inactivity upon attempting to log on or to start a job. The value takes into account the global SETROPTS INACTIVE setting and the last use date of the user.
Name	The name of the user if the **ACL id** is a user.
DfltGrp	The default connect group of a user. This field is found in USER profiles only.
RvC	This repeat field indicates whether the user has the REVOKE attribute in the connect group entry.
Instdata	The installation data for the user or group on the ACL.

REFRESH - Automatic refreshes for RACLIST, GENERIC checking, GLOBAL access checking, and WHEN(PROGRAM)

The SETROPTS REFRESH panel might be opened after a run if interactive changes were applied to any of the following:

- Profiles in classes that are RACLISTed.
- Generic profiles in classes that have GENERIC checking active.
- Global profiles describing classes for which global access checking is active.
- Program profiles if WHEN(PROGRAM) checking is active.

The SETROPTS refresh panel does not open in the following situations:

- The panel has been deactivated using the options available on the Setup Confirm panel. See "SE.4 Setup - Confirm" on page 1655.
- No SETROPTS commands were generated when changes were applied,
- The SETROPTS REFRESH commands were appended at the end of the CKRCMD file.

Figure 71 shows the SETROPS REFRESH pop-up that opens for confirming the commands.

```
zSecure Admin CONFIRM SETROPTS REFRESH  Press PF3 to accept
Complex DINO
  Refresh  Class    Also affected
/ GENERIC  APPCCLU
/ GENERIC  CA@MD    CA@APE $DATAMGR
/ GENERIC  DASDVOL  GDASDVOL
/ GENERIC  FIELD
/ GLOBAL   ACCTNUM
/ GLOBAL   DATASET
******************** BOTTOM OF DATA **********************
```

Figure 71. REFRESH Confirmation panel

The Confirm SETROPTS REFRESH panel presents a list of intended refresh commands. The list includes the refresh type along with the class to be refreshed when the commands run. If applicable, the class list includes other classes that share the same POSIT value and are also sensitive to this type of refresh and therefore affected when the commands run. If you do not want the Refresh command to be run for a specific entry, remove the selection by typing over the / value with a space. Use the scroll down function to review all the Refresh entries in the list. When you are done reviewing the Refresh commands, press **END** to run the Refresh commands for the selected classes.

The following refresh types can be performed:

GENERIC
Refresh the generic profiles

GLOBAL
Refresh the global access checking table

RACLIST
Refresh all profiles (for a RACLISTed class)

WHEN
Refresh WHEN class checking

After the REFRESH commands run, a browse panel opens to show the commands that were run and the result of the action.

RA.U USER - User information

The User Information panel provides access to simple selection functions for user profiles. Using these functions you can perform tasks such as the following:

- Add a new user profile from scratch. See "Add new user or segment" on page 105.
- Specify selection criteria for user profiles. Only profiles that match all criteria are selected. This selection effectively combines all the selection criteria with AND logic. Fields that are left blank are not tested.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Selection
Command ===> ____________________________________________________   _ start panel

_   Add new user or segment

Show userids that fit all of the following criteria
Userid  . . . . . . C##QA0*___    (user profile key or filter)
Name  . . . . . . . ____________________________ (name/part of name, no filter)
Installation data . ____________________________ (data scan, no filter except *)
Owned by  . . . . . ________     (group or userid, or filter)
Default group . . . ________     (group or filter)
Connect group . . . ________     (group or filter)

Additional selection criteria
_  Other fields      _  Attributes       _  Segment presence  _  Absence

Output/run options
/  Show segments     /  All              _  Specify scope
_  Print format      _  Customize title  _  Send as email
   _  Background run _  Full page form   _  Sort differently  _  Narrow print
```

Figure 72. Simple user selection screen

For example, you can find all user IDs that have *C##QA0*in the first six positions by typing *C##QA0** in the **Userid** field. The other fields work similarly.

The following simple selection criteria are supported:

Table 34. Simple Selection Criteria

Selection criteria	Description
Userid	This ID, or a matching ID if a filter is used.
Name	Search for the specified string in any position within the name field. You cannot use a filter in this field. A *substring scan* is performed.
Installation data	Find occurrence anywhere in the installation data. You cannot use a filter in this field. When this command runs, a *substring scan* is performed.
Owned by	Search for the specified OWNER. The owner can be a user or group.
Default group	With the following default group.
Connect group	Connected to the specified group.

Additional selection criteria can be requested through the following options which can be selected by entering **/** or **S** in the entry field.

Table 35. Additional Selection Criteria

Selection criteria	Description
Other fields	Use this field for selecting on date fields, complex name, schedule name, or password interval. The selection panel is shown in "Additional selection - Other fields" on page 98. If the field is not selected, the **Other fields** selection criteria are ignored. However, the settings are saved for later use as long as you are using the **RA.U** option.
Attributes	For selecting on the following fields: • Security attributes like special, operations, auditor, revoked, inactive, protected, restricted, and `UAUDIT`. • Presence of logon restrictions, certificates, `raclinks`, and `userdata`, • `CKGRACF` dual or triple authority and queued commands. • User security attributes like special, operations, auditor, revoked, inactive, protected, restricted, `UAUDIT`, and queued commands. The selection panel is shown in "Additional selection - Attributes" on page 101. If the field is not selected, the **Attributes** selection criteria are ignored. However, the settings are saved for later use as long as you are using the **RA.U** option.
Segment presence	If this field is selected, criteria can be specified for the presence of application segments. A segment selection panel and a segment field selection panel are shown. Unless the output option **Show segments** has also been selected, these panels only show the base segment of groups that have the specific non-base segment. If the field is not selected, the selection criteria are not used but are saved for later use as long as you remain in **RA.U**.
Segment absence	If this field is selected, absence of a segment can be specified as an additional selection criterion. If the field is not selected, the selection criteria are not used but are saved for later use as long as you remain in **RA.U**.

Table 36 lists the output and run options you can specify.

Table 36. Output and Run options

Show segments	Show a selectable set of application segments for specifying select and exclude criteria based on segment field values. If this option is not selected, the segment subset is not used but is saved in your ISPF profile for later use. This flag setting is saved in your ISPF profile.
All	Select this option with the *Show segments* to show all segments for the selected users.
Specify scope	If this field is selected, you can limit the results to the scope of a user ID or group.
Print format	If this field is selected, the results are provided is in print format instead of an ISPF display. This flag setting is saved in your ISPF profile and is shared between all **RA** options showing it. The other print-related options only apply if this one has been selected. See also "Print format" on page 113.
Customize title	If this field is selected together with *Print format*, you can change the subtitle for the selection and add an extra title that is saved in your ISPF profile. For example, you might specify a title that shows your company name, department, and phone number. This flag setting is saved in your ISPF profile and is shared between all RA options showing it.

Table 36. Output and Run options (continued)

Send as email	If this field is selected along with **Print format**, then a panel opens for specifying the email address destination for the report. The email function does not work until you have configured the SMTP options with `SETUP OUTPUT`. This flag setting is saved in your ISPF profile and is shared between all `RA` options showing it.
Background run	If this field is selected together with **Print format**, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared by all `RA` options showing it.
Full page form	If this field is selected together with *Print format*, then the report format uses at least one full page per user for the user detail information. This flag setting is saved in your ISPF profile. If you have requested segments, they are shown on the same page with the other user ID information. If the *Full page form* field is not selected, each segment type is shown in its own tabular report.
Sort differently	If this field is selected together with *Print format*, then an alternate sort order can be selected. If you want to change the sort order in an ISPF display (Print format not selected), you can use the SORT primary command in the actual display. This flag setting is saved in your ISPF profile.
Narrow print	If this field is selected together with *Print format*, then the width of the page is limited to 79 characters, independently of the actual print file record length. If the field is not selected, then the page layout you specify must support a width of 132. However, the length can extend beyond that if the print file has a larger record length. This flag setting is saved in your ISPF profile and is shared between all panels displaying this option.

User profile tabular display

A user information panel is shown in Figure 73.

```
zSecure Admin USER overview                                    Line 1 of 4
Command ===>                                                   Scroll===> CSR
Users like C##QA0*                                 5 Sep 2000 14:18
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ C##QA001 DINO     QA SUBJECT 001______ C##QA___ C##QA___ ____ ___       X   2
__ C##QA002 DINO     QA SUBJECT DUAL AUTH C##QA___ C##QA___ ____ ___ g     X   2
__ C##QA003 DINO     QA SUBJECT 003______ C##QA___ C##QA___ ____ ___       X   1
__ C##QA004 DINO     QA SUBJECT 004______ C##QA___ C##QA___ RI__ ___       X   1
******************************* BOTTOM OF DATA ********************************
```

Figure 73. User profile display

Table 37 describes the columns on this panel.

Table 37. User profile tabular display - Column descriptions

Column name	Description
User	RACF user profile name (user ID).
Complex	Name for the RACF security database containing this profile.
Name	Programmer name field of RACF profile. Users can change their own programmer name field.
DfltGrp	Default group for the user. Users can change their own default group. The user can only change the default group to a group that is already connected.
Owner	The owning user or group for the user profile.

Table 37. User profile tabular display - Column descriptions (continued)

Column name	Description
RIRP	Indicates the user status: **R** revoked. **I** due to be revoked through inactivity, **R** restricted, which means that access through the UACC, global, and ID(*) are not honored. **P** protected, which means that user ID cannot be used to logon.
SOA	Indicates the user attributes, Special, Operations, or Auditor.
gC	The **g** column indicates that the user is connected to at least one group with the Special, Operations, or Auditor attribute. The **C** column indicates that the user has at least one class authorization.
LCX	**L** indicates at least one RACLINK. **C** indicates a user certificate. **X** indicates an expired password.
Grp	Number of groups that the user is connected to.

You can scroll the panel to the right to view additional information as shown in Figure 74.

```
zSecure Admin USER overview                                    Line 1 of 4
Command ===>                                                     Scroll===> CSR
like C##QA0*                                        12 Sep 2009 14:18
   User      LastCon    LastUse   time   LastPwd   LastPhrChg PwInt Eff LogDays
__ C##QA001  09Sep2009  09Sep2009 03:45  04Aug2009               __90  90 SMTWTFS
__ C##QA002  10Sep2009  10Sep2009 03:09  04Aug2009               __90  90 SMTWTFS
__ C##QA003  29Mar1997  29Mar1997 10:15  29Mar1997               __30  30 SMTWTFS
__ C##QA004  13Jun2008  13Jun2008 06:16  24Apr2008               __90  90 SMTWTFS

****************************** BOTTOM OF DATA ******************************
```

Figure 74. User profile display (second screen)

Table 38 describes the columns that display when the panel is scrolled to the right.

Table 38. User profile tabular display - Column descriptions (scroll right)

Column name	Description
LastCon	Last logon date (with any of the current connect groups)
LastUse	Last logon or update date.
time	Last logon or update time.
LastPwd	Last password change. Empty means never.
LastPhrChg	Last password phrase change. Empty means never.
PwInt	Password interval in days.
Eff	Effective password interval in days. This value combines the **PwInt** column with the system-wide password interval setting.
LogDays	Days that logon is permitted.

You can scroll the panel to the right again to view additional information as shown in Figure 75.

```
zSecure Admin USER overview                                    Line 1 of 4
Command ===>                                                     Scroll===> CSR
like C##QA0*                                        5 Sep 2000 14:18
   User      LogTime   U CreateDat SecLabel RevokeDate  ResumeDate  ClAut Link
 __ C##QA001 _________ _ 10Dec2000 ________ ___________ ___________  0    0
 __ C##QA002 _________ _ 16Oct2001 ________ ___________ ___________  0    1
 __ C##QA003 _________ _ 20Jan2009 ________ ___________ ___________  0    0
 __ C##QA004 _________ _ 20Jan2009 ________ ___________ ___________  0    0

****************************** BOTTOM OF DATA ********************************
```

Figure 75. User profile (third screen)

Table 39 describes the columns that display when the panel is scrolled to the right again.

Table 39. User profile tabular display - Column descriptions (scroll right, second time)

Column name	Description
LogTime	Times that logon is permitted.
U	User must be audited (UAUDIT attribute).
CreateDat	Creation date of the profile.
SecLabel	Security label.
RevokeDate	Date on which the user is to be revoked
ResumeDate	Date on which the user is to be resumed
ClAut	Number of class authorities the user has.
Link	Number of user IDs the user is linked to through RACLINK.

The display can be scrolled right a third time to see the installation data.

```
zSecure Admin USER overview                                    Line 1 of 5
Command ===>                                                     Scroll===> CSR
like C##QA0*                                        5 Sep 2000 14:18
    User     #Cert #Maps EPEM AG Pri InstData
__ C##QA001      0     0  Y Y    __  ____________________________________________________
__ C##QA002      0     0         __  ____________________________________________________
__ C##QA003      0     0         __  ____________________________________________________
__ C##QA004      0     0         __  ____________________________________________________
__ C##QA005      0     0         __  QA SUBJECT 005 O.A. TEST G0028 G0029 G0030 G0031 G0032 G003
```

Figure 76. User profile tabular display (second screen)

Table 40 describes the columns that display when the panel is scrolled to the right again.

Table 40. User profile tabular display - Column descriptions (scroll right, third time)

Column name	Description
#Cert	Number of digital certificates defined for this user.
#Maps	Number of identity mappings that map to this user
E	This flag field indicates that the user profile contains a password envelope with a two-way encrypted form of the password.
P	This flag field indicates that the user ID can use a password phrase to logon.

Table 40. User profile tabular display - Column descriptions (scroll right, third time) (continued)

E	This flag field indicates that the user profile contains a password phrase envelope with a two-way encrypted form of the password phrase.
M	This flag field indicates that password checks for the user are case-sensitive.
AG	Indicates that the user has the `ADSP` or `GRPACC` attributes. These attributes are deprecated. Do not use them unnecessarily.
Pri	The relative audit priority for this user ID.
InstData	Installation data of this user.

User profile detail display

Select any user on the user profile table display to see the detail view. To select an entry, place the cursor on the first character of row selection field, then press Enter, or type *S* in the input entry field. Then, press **Enter**.

```
zSecure Admin USER overview                                  Line 1 of 45
Command ===>                                                   Scroll===> CSR
like C##QA0*                                      5 Sep 2000 14:18

_ Identification of C##QA001                                          DINO
  User name                     QA SUBJECT 001______
  Installation data             ________________________________________
_ Owner                         C##QA___                    Q.A. TESTSUBJECTS
_ User's default group          C##QA___                    Q.A. TESTSUBJECTS

  Group    Auth    R SOA AG Uacc    Revokedt    Resumedt    InstData
_ C##QA___ CONNECT _ ___ __ NONE___ __________ _________ Q.A. TESTSUBJECTS
_ C##CXCNG USE____ _ ___ __ NONE___ __________ _________ TEST GROUP DOR CNGR

  System access                             Statistics
  Revoked (may be by date)      No_         Creation date      18Jul96
  Inactive, revoked or pending  No          Last RACINIT current connects 20Jul00
  Days of week user can logon   SMTWTFS     User's last use date         20Jul00
  Time of day user can logon    _________   User's last use time          18:51
  Date user will be revoked     __________  (ddmmmyyyy or NOREVOKE)
  Date user will be resumed     __________  (ddmmmyyyy or NORESUME)

  Password                                  Password phrase
  Has a password                Yes         Has a password phrase         Yes
  Expired password              No          Expired password phrase       No
  Password changed date         23Mar06     Password phrase change date   23Mar06
  Password expiration date      21Aug06     Password phrase expiry date   21Aug06
  Old passwords present #         1         Old pass phrases present #    2
  Password interval             _90         Has a passw. phrase envelope
  Password interval in effect    90         Failed password attempts #    0
  Mixed case password           Yes
  Has a password envelope
  Password disabled   PROTECTED No_

  Mandatory Access Control                  Privileges
  Security label                ________    Security admin        SPECIAL No
  Security level                            DASD administrator OPERATIONS No
  Categories list                           Global audit set/list AUDITOR No
                                            Class authority               ________

  Safeguards
  Ignore UACC/Glob/* RESTRICTED No_
  Log all user actions   UAUDIT No_

  Linked node.user Type    Stat Pwd  Defined (GMT)    Approved (GMT)   Creator
_ DINO.C##QAWT     Peer    Sync ___  1998/09/10 11:09 1998/09/10 11:26 C##QA001
  Digital certificate labels       Digital certificate names
  Primary_____________________     6F.Jones@Zsecur.NL.CN=Root.OU=CryptoLab.O=Co
  Certificate filter label
  _____________________________
  Identity mapping label Identity mapping filter                        Identity
  _ myFirstRACMAP        UID=armeBert,OU=Tools Development,O=IBM,C=NL  ldaps://
  UsrNm   Flg UsrData
_ PHONE    00 +31-15-2513333
  CKGRACF authority requirement
_ Authority setting DUAL set by C##BGUI at 18 Nov 1997 16:00
  Scheduled events
_ Scheduled event: Schedule 'QA#UIT' disable  2 Sep 2001; set by C##QA1G at  2
_ Queued command (R): USER C##QA001 SCHEDULE HELPDESK ENABLE (01Mar2002:02Mar20
  Inactive commands
_ Queued command (E): USER C##QA001 SCHEDULE HELPDESK DISABLE (30Aug2000:31Aug2
  Commands that have been executed
_ Queued command (CA): USER C##QA001 SCHEDULE QA#UIT DISABLE (02Sep2000); reque
  Other CKGRACF data
_ Default password set by C##BLU1 at  5 Nov 1998 09:37
****************************** BOTTOM OF DATA ********************************
```

Figure 77. User profile detail display panel

Depending on SETUP options and data availability, the following fields of interest can be shown.

Identification fields

Table 41. User profile detail display - Identification section field values

Field	Description
Identification of	This header line contains the user ID and (far to the right) the complex name.
User name	The name (*programmer name*) of the user. Users can change their own *programmer name* field.
Installation data	Installation data field of the profile.
Owner	The owning group or user ID and is (on the detail display) optionally followed by the owning user name and installation data or the group installation data.
User's default group	The default connect group and is (on the detail display) optionally followed by the group installation data. Users can change their own default group. The user can only change the default group to a group that is already connected to.

Connect group fields

Depending on SETUP options, and data availability. The following fields of interest can be shown.

Table 42. User profile detail display - Connect group field values

Field	Description
Group	The groups the user is connected to
Auth	Connect authority
R	Indication whether this connect is revoked. This value takes into account any revoke and resume dates and the database *dumpdate*.
SOA	Indication whether user has the group SPECIAL, OPERATIONS, or AUDITOR attributes.
AG	Settings used for new data set or resource profiles created while the user is logged on with this group as the current connect group. **A** for ADSP is only used if the system-wide SETROPTS ADSP option has also been set. It controls whether data set creation automatically creates a discrete data set profile. The use of this attribute is deprecated. The G for GRPACC regulates whether the group must be added with UPDATE access to new group DATASET profiles.
Uacc	Default universal access for new dataset / resource profiles created while the user is logged on with this group as the current connect group.
Revokedt	Revoke date of connect
Resumedt	Resume date of connect
InstData	Installation data field of the group

System access fields

Field	Description
Revoked (can be by date)	Whether the user is in revoked status at the time of the database unload. This value is determined based on the revoke and resume dates for the user schedule.

Field	Description
Inactive, revoked or pending	This field shows *Yes* if the user ID cannot logon because of inactivity. It can be pending revoke, or already revoked (if the user has already tried to logon).
Days of week user can logon	1letter per day of the week, starting with Sunday. This field contains *SMTWTFS* if the user can logon on any day of the week.
Time of day user can logon	Indicates when a user can logon. The value can be blank if the logon time is not restricted, or a time range *HHMM:HHMM* if there is a restriction on the local time of day.
Date user will be revoked	The revoke date for the user ID.
Date user will be resumed	The resume date for the user ID

Statistics section

Field	Description
Creation date	This is the date that the profile was created.
Last RACINIT current connects	The last RACINIT logon or job initiation date with any of the current Connects for the user. This value is the last logon date if no connects have been removed. In that case it is often more accurate than the last use date.
User's last use date	The last use date. This value is usually the last RACINIT date, but it is also updated for certain user profile updates
User's last use time	The time of day of the last use. See also **User's last use date**.

Password fields

Field	Description
Has a password	This flag field indicates that the user can use a password to logon.
Expired password	This field contains *Yes* if the password is currently expired, which means that the user must change the password at the next login.
Password changed date	The date of the last password change
Password expiration date	The expiration date for the user password. The user must change the password when logging in on or after this date.
Old passwords present #	Number of previous passwords.
Failed password attempts #	Contains the number of failed passwords attempts since the last successful logon.
Password interval	The current password interval value. See the **Password interval in effect** field description for the value that is currently used by the system.
Password interval in effect	The password interval for the user ID that is currently active in the system (in days, or blank for NOINTERVAL). This value is also influenced by the SETROPTS INTERVAL setting.
Mixed case password	This flag field indicates that password checks for the user are case-sensitive.

Field	Description
Password disabled PROTECTED	Shows *Yes* if the user cannot be used with a password or revoked due to invalid passwords.
Has a password envelope	This flag field indicates that the user profile contains a password envelope with a two-way encrypted form of the password.

Password phrase

Field	Description
Has a password phrase	This flag field indicates that the user can use a password phrase to logon.
Expired password phrase	This field contains *Yes* if the password phrase is currently expired. If it is expired, the user must change the password at the next login.
Password phrase change date	The date of the last password phrase change.
Password phrase expiry date	The date the user password phrase expires. The user must change the password phrase when logging in on or after this date.
Old pass phrases present #	Number of previous password phrases.

Mandatory Access Control fields

Security label	Contains the default security label used in Mandatory Access Control decisions (B1 security).
Categories list	Lists all security categories that the user is permitted to read.

Privileges fields

Security admin SPECIAL	Contains *Yes* if the user has system-wide SPECIAL authority, which is usually an attribute that applies to a a central security administrator.
DASD administrator OPERATIONS	Contains *Yes* if the user has system-wide OPERATIONS authority, which means that the user ID can be used for changing almost any data set and for performing DASD management operations.
Global audit set/list AUDITOR	Contains *Yes* if the user has system-wide AUDITOR authority, which indicates that the user can review all security settings and request audit logging.
Class authority	The names of the general resource classes that the user can define new profiles for, or refresh profile caches in-storage.

Safeguards

Ignore UACC/Glob/* RESTRICTED	This field indicates whether user ID has the RESTRICTED attribute. If the value is *YES*, the UACC, global access, and ID(*) permits do not apply.
Log all user actions UAUDIT	This field contains *YES* if the user has the UAUDIT attribute. This attribute specifies all actions that are logged to SMF.

RACLINK section

Field	Description
input field	You can use the input field for a RACLINK entry to manage RACLINK associations. This field accepts the following line commands: **A** (Approve), **C** (Copy), **D** (Delete), or **I** (Insert) a RACLINK. For details, see "RACLINK fields" on page 79.
Linked node.user	Partner user ID at the specified node that this user is linked to through a `RACLINK` association. Authorized users can edit this field to change the value. Specify the value using the following syntax: `[node].user` The *node* can be either empty or a node name. The *user* is the `userid` for a valid user profile. Both values can be a maximum of 8 characters.
Type	Specifies the type of association between user IDs. Authorized users can edit this field to change the value. The following values are accepted. • *P*, *Peer*, or blank specifies peer association between users, with or without password synchronization. • *Managed* association. Password synchronization is not permitted.
Stat	Link status. This value is normally blank which indicates an approved status. However, the value can also be *Err* in case of an error, or *Pend* if pending approval. If the status is Pend, the association record can be approved using the **A** line command. For details, see "RACLINK fields" on page 79.
Pwd	Password synchronization flag, either *Sync* (active) or blank. Authorized users can edit this field to change the value. This field is only meaningful for RACLINK associations with `Type=Peer`. The field can have the following values: • *S* or *Sync* specifies association with password synchronization. • Leaving the field blank specifies association without password synchronization.
Defined (GMT)	Timestamp when link was defined.
Approved (GMT)	Timestamp when link was approved
Creator	User that created the link

Additional, optional properties

Digital certificate labels	List of associated digital certificates by label
Digital certificate names	List of associated digital certificates by name. Each entry lists the **Serial Number** and **Distinguished Name** for the Issuer, separated by a dot.
Certificate filter label	List of labels describing the digital certificate filters that map to this user ID.
Identity mapping label	The labels for the identity mappings to this user ID.

Identity mapping filter	The identity filter for the identity mappings to this user ID. The value can be in X.500 format.
Identity mapping registry	The registries for the identity mappings to this user ID.
Mapping profile label	Mapping profile name.
Audit concern	A concatenation of audit concerns for the user ID.
UsrNm	The names of the `userdata` fields, excluding those fields used by `CKGRACF`.
Flg	Flag associated with the `userdata` field
UsrData	Contents of the `userdata` field
CKGRACF authority requirement	The authority required to change this USER profile via `CKGRACF` (SINGLE, DOUBLE or TRIPLE), that is, the number of administrators who must sanction a command.
Scheduled events	The events making up the schedules deciding when the user can enter the system
Commands requiring administrator action	The commands that have not been fully authorized yet as per the `CKGRACF` authority requirement as specified in the **CKGRACF authority requirement** or through the system-wide default.
Inactive commands	Requested commands that were not fully authorized before they expired were withdrawn or denied. Inactive commands are listed as part of the audit trail.
Commands that have been executed	Commands that were fully authorized and run. These commands are included in the audit trail.
Other CKGRACF data	`Userdata` fields used by `CKGRACF` for other purposes. For user profiles, this value only shows the presence of a default password.

For more information, see the following topics:

- "RA.2 QUEUED - Queued commands" on page 185
- "MR - CKGRACF mulitple authority requirement" on page 63
- "MS - CKGRACF revoke/resume schedules" on page 64
- "P - Change password and resume user" on page 67

Additional selection - Other fields

If you check the 'Other fields' option on the primary selection panel, the advanced selection panel shown in Figure 78 on page 99.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Selection
Command ===>
Users like C##QA0*
Specify additional selection criteria:
Selection by date
Last logon/connect. __   ________________      (operator: < <= > >= = <> ¬= )
Last logon/update . __   ________________      (date: yyyy-mm-dd, ddMMMyyyy
Password changed  . __   ________________       NEVER, DUMPDATE, DUMPDATE-nnn,
Pass phrase changed __   ________________       DUMPDATE-INACTIVE, TODAY,
Creation date . . . __   ________________       TODAY-nnn, TODAY-INACTIVE)
Revoke date . . . . __   ________________

Logdays selection
_  Sun     _  Mon     _  Tue     _  Wed     _  Thu     _  Fri     _  Sat

Miscellaneous fields
Password interval . __ ___      (operator+number or Y/N)  / Effective only
Schedule name . . . ________    (schedule name or filter)
Complex . . . . . . ________    (complex name or filter)
```

Figure 78. Advanced user selection

Use this selection panel to specify a comparison criterion using the last connect date, last use date, last password change date, creation date, or revocation date, and to select on the presence or absence of certain attributes. The password interval field can be used either for a comparison or as an attribute that indicates if the users have any interval or NOINTERVAL.

The following advanced selection criteria are supported:

Table 43. Advanced user selection criteria

Selection Criteria	Description
Last logon/connect	Test the last connect RACINIT date, use with comparison operators, or NEVER. This value is the last logon date if no connects have been deleted.
Last logon/update	Test the date of the last RACINIT or update, use with comparison operators, or NEVER. This value can be more recent than the last logon date if the user profile has been updated.
Password changed	Test the date the password was last changed, *NEVER*, or < DUMPDATE-*nn* identifies users that have not changed their password in the last *nn* days.
Pass phrase changed	Test the date the password phrase was last changed, NEVER, or < DUMPDATE-*nn* to find users that have not changed their password phrase in the last *nn* days.
Creation date	Test the day the user was defined to RACF.
Revoke date	Revoked explicitly, or to be revoked on the specified date.
Logdays selection	Selects user IDs based on days they can logon (LOGDAYS). You can specify the following values. *Y* for all user IDs that are permitted to logon on the selected day. You can specify *S* or / instead of *Y*. *N* - for all user IDs that are not permitted to logon on the selected day blank - no selection is performed for this day

Table 43. Advanced user selection criteria (continued)

Selection Criteria	Description
Password interval	Test the password interval length. Specify *Y* to select only users with an expiring password. Specify *N*to select only users with a non-expiring password. Leave this field blank to disregard the password interval when making selections.
Effective only	When this option is selected, the value entered for the password interval (PASSINT field in the USER profile) is compared to the value of the SETROPTS PASSWORD(INTERVAL()) setting and the smaller value is used as the effective password interval. If the value of the effective password interval is smaller than the PASSWORD(MINCHANGE()) value, the PASSWORD(MINCHANGE()) value becomes the effective password interval. **Note:** The option has no effect on userids with passwords that cannot be changed; for example, userids assigned the PROTECTED attribute.
Schedule name	CKGRACF schedule name or a filter.
Complex	In a complex with this name, or a matching complex if a filter is used.

It is possible to test on the contents of DATE fields using the comparison operators listed on the panel. The operators have the following meaning:

Table 44. Date comparison operators for advanced user selection criteria

Operator	Description
<	Date is before the specified value.
>	Date is after the specified value.
=	Date is at the specified value.
<> or ¬=	Date is not at the specified value.

Table 45 lists the valid formats for a DATE comparand. You can specify the format in either upper or lower case.

Table 45. Date comparand formats for advanced user selection criteria

Date comparand	Description
ddmmmyyyy	**Example:** 01JAN1998. Valid month codes are *JAN*, *FEB*, *MAR*, *APR*, *MAY*, *JUN*, *JUL*, *AUG*, *SEP*, *OCT*, *NOV*, *DEC*.
yyyy-mm-dd	**Example:** 1998-12-31. This is the ISO date format.
NEVER	Indicates that the field has never been set, or has been reset to its initial state. For example, Last logon = NEVER looks for users who have never logged on (LJDATE). *NEVER* is only useful when used with the = operator.
DUMPDATE	The date when the UNLOAD you are processing was created or, if you are working from the active RACF database, today.

Table 45. Date comparand formats for advanced user selection criteria (continued)

Date comparand	Description
TODAY	Keyword to represent the current date.
DUMPDATE-nnn *TODAY-nnn*	*nnn* days before *TODAY* or *DUMPDATE*. If you are working with an UNLOAD data set created in the past, do not use the *TODAY* value in your compare specification.
DUMPDATE-INACTIVE *TODAY-INACTIVE*	The SETROPTS INACTIVE interval before *DUMPDATE* or *TODAY*.
DUMPDATE+nnn TODAY+nnn	*nnn* days after *TODAY* or *DUMPDATE*. This value is useful for finding REVOKE actions.

Figure 79 shows a query to select users that had group authorization SPECIAL and OPERATIONS attribute in any group, no password interval, and had not changed their passwords for at least 60 days since the date the currently selected database image was captured (*dumpdate - 60*).

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                       zSecure Suite - RACF - User Selection
 Command ===>
 Users like C##QA0*
 Specify additional selection criteria:
 Selection by date
 Last logon/connect. __   ________________      (operator: < <= > >= = <> ¬= )
 Last logon/update . __   ________________      (date: yyyy-mm-dd, ddMMMyyyy
 Password changed  . <_   dumpdate-60_____       NEVER, DUMPDATE, DUMPDATE-nnn,
 Pass phrase changed __   ________________       DUMPDATE-INACTIVE, TODAY,
 Creation date . . . __   ________________       TODAY-nnn, TODAY-INACTIVE)
 Revoke date . . . . __   ________________

 Logdays selection
 _  Sun    _  Mon    _  Tue    _  Wed    _  Thu    _  Fri    _  Sat

 Miscellaneous fields
 Password interval . __  N__                   (operator+number or Y/N)
 Schedule name . . . ________    (schedule name or filter)
 Complex . . . . . . ________    (complex name or filter)
```

Figure 79. Advanced user query

Additional selection - Attributes

If you check the Attributes option on the primary selection panel, the advanced selection panel shown in Figure 80 on page 102 is displayed.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - User Attributes
Command ===>
Users like C##QA0*
Specify groups of criteria that the userids must meet:
Systemwide and group authorizations
OR_    _   Special       _   Operations    _   Auditor      _   Class auth
       _   Group-special _   Group-oper    _   Group-audit

Logon status
OR_    _   Revoked       _   Inactive      _   Protected    _   Passw expired
       _   Revoked group _   Certificate   _   Pass phrase  _   Phrase expired
       _   When day/time

User properties
OR_    _   Has RACLINK   _   Restricted    _   User audited _   Mixed case pwd

CKGRACF features
OR_    _   Queued cmds   _   Schedules     _   Userdata     _   MultiAuthority

Connect authority . >=_  2_  1. Use   2. Create   3. Connect  4. Join
```

Figure 80. User attribute selection

Use this selection panel to select on the presence or absence of certain attributes. Some of the attributes are grouped. You can specify whether you want them combined with AND or OR logic within the group. All resulting clauses are furthermore combined with AND logic.

Table 46 lists the advanced selection criteria that are supported. For each selection criteria field, you can specify the following values:

- *Y* or / selects based on the criteria being true.
- *N* selects based on the criteria being false.
- If you leave the selection field blank, that selection criteria is ignored during the selection process.

Table 46. Advanced selection criteria for User attributes

Field	Description
System-wide and group authorizations: Special, Operations, Auditor, Class auth	Selects record based on the system-wide and group authorization attributes: SPECIAL, OPERATIONS, and AUDITOR.
Logon status: Revoked	Selects based on whether the ID has been revoked.
Logon status: Inactive	Selects based on whether the ID is inactive. Inactive users are those who have been logged on for too long based on the setting specified by SETROPTS INACTIVE() option.
Logon status: Protected	Selects based on whether a user ID has the PROTECTED attribute.
Logon status: Passw expired	Selects based on whether the password for the user ID is expired.
Logon status: Revoked group	Selects based on whether the user has a revoked group connect.
Logon status: Certificate	Selects based on whether the user has a security certificate.
Logon status: Pass phrase	Selects based on whether the user requires a password phrase.
Logon status: Phrase expired	Selects based on whether the user password phrase is expired.

Table 46. Advanced selection criteria for User attributes (continued)

Field	Description
Logon status: When day/time	Selects based on whether the user has logon restrictions by date or time.
User properties: Has RACLINK	Selects based on whether the user ID is linked to another user ID or database.
User properties: Restricted	Selects based on whether a user ID has the `RESTRICTED` attribute. Non-restricted users have access to the UACC, global, and `ID(*)` resources.
User properties: User audited	Selects based on whether a user is being audited which is indicated by the status of the UAUDIT attribute.
User properties: Mixed case pwd	Select based on whether a user ID has a mixed case password.
CKGRACF features: Queued cmds	Select based on whether the command queue contains commands for the user ID.
CKGRACF features: Schedules	Select based on whether a user ID has any scheduled events.
CKGRACF features: Userdata	Selects based on whether user has any non`CKGRACF userdata`.
CKGRACF features: MultiAuthority	Selects based on whether a user ID has dual or triple authority requirements.
Connect authority	Selects a user based on the specified connect authority. Only users that have at least one group connection that satisfies the authority-level comparison condition will be shown.

In Figure 81, a query is shown after users that had group-special `OR` group-operations authorization (in any group).

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Attributes
Command ===>
Users like C##QA0*
Specify groups of criteria that the user IDs must meet:
Systemwide and group authorizations
OR_     _   Special         _   Operations    _   Auditor      _   Class auth
        /   Group-special   /   Group-oper    _   Group-audit

Logon status
OR_     _   Revoked         _   Inactive      _   Protected    _   Passw expired
        _   Revoked group   _   Certificate   _   Pass phrase  _   Phrase expired
        _   When day/time   _   ID mapping

User properties
OR_     _   Has RACLINK     _   Restricted    _   User audited

CKGRACF features
OR_     _   Queued cmds     _   Schedules     _   Userdata     _   MultiAuthority
```

Figure 81. User attribute query

Line commands on a User profile display

On any profile level display, the line command **/** is available. You can use this command to query what other line commands are available on a line, as shown in Figure 82 on page 104.

```
zSecure Admin USER Overview                                    Line 1 of 3
Command ===>                                                    Scroll===> CSR
like C##QA* with password changed < DUMPDATE-60 26 Nov 1998 07:47
   Profile  Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ C##QAP0  DD981126 PROTERM TEST RUNNER1 C##QA___ C##QA___ ____ ___ g        6
__ C##QA1A  DD981126 QA SUBJECT CNG ADMIN C##QA___ C##QA___ ____ ___ g    X   1
/_ C##QA1G  DD981126 QA SUBJECT + GRPSPEC C##QA___ C##QA___ ____ ___ g        1
****************************** BOTTOM OF DATA ********************************
```

Figure 82. User Overview panel

When you enter the / command on any line, a pop-up opens to describe the available line commands. You must scroll up and down to see all available line commands. The line commands available for a USER profile display are shown in the Table 47.

Table 47. Line commands for User profile display

Command	Meaning	Explanation
A	Authorization (permits and scope)	"RA.3.4 Permit/Scope - Report access of a user or group" on page 207
AC	Access Check for user ID on one profile	"RA.1 ACCESS - Access Check" on page 184
C	Copy user ID	"C - Copy" on page 55
CO	Add connect	"CO - Add connect" on page 57
D **DD**	(Prepare actions for) delete user ID, or delete a non-base segment	"D - Delete" on page 58
E	Display event logging	"E - Event" on page 59
L	RACF `listuser` all command	The output of the `listuser` command is presented in a browse panel.
M	Move user from group (to another)	"M - Move a user to another group" on page 60
MI	Manage user ID-information	"MI - Manage information" on page 61
ML	Manage logon-information	"ML - Manage logon information" on page 61
MR	Manage CKGRACF authority requirements	"MR - CKGRACF mulitple authority requirement" on page 63
MS	Manage CKGRACF revoke/resume schedules	"MS - CKGRACF revoke/resume schedules" on page 64
MT	Manage TSO-information	"MT - Manage TSO information" on page 66
MU	Manage installation-defined USERDATA	"RA.3.9 USERDATA - User data management" on page 219
P	Change password and resume	"P - Change password and resume user" on page 67
PE	Add or delete permit	"PE - Add or delete permit" on page 69
R **RR**	Recreate user ID	"R - Recreate a profile" on page 70
S	Show additional information	"S - Select" on page 72

Table 47. Line commands for User profile display (continued)

Command	Meaning	Explanation
SE	Show application segments	"SE - Show application segments" on page 72 and "Application segments" on page 106.
SR	Show all relevant information	"SR - Show all Relevant information" on page 73
TR	Trust bestowed on user ID	"TR - Trust bestowed on userid" on page 74
X **XX**	Exclude user ID from FORALL processing	"X - Exclude profile line command" on page 74
Z **ZZ**	Select user ID for FORALL processing	"Z - Select a profile" on page 74
34	Dataset List Utility	"34 - Data set list utility" on page 74

The line commands available on the detail display differ per field:

- For the connect groups, the line commands **L** (List), **C** (Copy) and **D** (Delete) are supported. These commands issue the RACF `listgrp`, `connect`, and remove commands. See "Connect detail view" on page 77.
- For digital certificates, the line commands **L** and **D** are supported, resulting in different forms of the RACDCERT command. See "Digital Certificate detail view" on page 78.
- For RACLINK associations, the line commands **A** (Approve), **C** (Copy), **D** (Delete), **I** (Insert). See "RACLINK fields" on page 79.
- For installation-defined `userdata` fields, the line commands **C** (Copy) and **D** (Delete) are supported, resulting directly in CKGRACF commands. The **I** (Insert), **R** (Repeat) and **S** (Select) commands are also supported. For more information about CKGRACF `userdata` fields and supported line commands, see See "USR fields" on page 78.
-

  "Access List detail view" on page 75

  "Connect detail view" on page 77

  "Data set detail view" on page 78

  "Digital Certificate detail view" on page 78

  "USR fields" on page 78

  "RACLINK fields" on page 79

Add new user or segment

You can add a new, generic user profile, or empty segment to the current system with the **Add new user or segment** option on the RACF User Selection panel ("RA.U USER - User information" on page 87).

You can also add a new user by copying an existing one. For details, see "C - Copy" on page 55. If you want to add a dataset profile or segment on another system, you must use a batch job.

Use the following procedure to add a new user profile or segment from the RACF User Selection panel.

1. On the RACF User Selection panel (Figure 72 on page 87), type a / or *S* in the **Add new user or segment** field.

2. Press **Enter** to open the User Add panel.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Add
Command ===> ____________________________________________________________

Userid  . . . . . . C##QA99_ (required)
Default group . . . C##QA___ (required for new userid)
Password  . . . . .          . . .          (twice, required for new userid)
Owned by  . . . . . C##QA___ (may also be set in the follow on update dialog)
Password phrase . . ____________________________________________________
_____________________________________ (9-100 chars, in single quotes)

/   Define new userid

_   Add CICS segment                  _   Add NDS segment
_   Add CSDATA segment                _   Add NETVIEW segment
_   Add DCE segment                   _   Add OMVS segment
_   Add DFP segment                   _   Add OPERPARM segment
_   Add EIM segment                   _   Add OVM segment
_   Add KERB segment                  _   Add PROXY segment
_   Add LANGUAGE segment              _   Add TSO segment
_   Add LNOTES segment                _   Add WORKATTR segment
```

Figure 83. ADD USER panel

3. On the Add panel, you can add a new user profile, add an empty segment, or add a combination of a user profile and segment. For information on performing these tasks, see the ISPF panel help.
4. After specifying the field information, press **Enter** to the immediately add the user profile or segment on the system where you are logged on.

   The RACF command response is only shown if there is a nonzero return code.

Notes:

1. Your ISPF profile stores the default group and owner based on previous additions for users that do most of their additions in the same group. The format of the display is the same as the detail display described in "User profile detail display" on page 92.
2. Security zSecure requires users to type a new password twice for added security.
3. Users cannot specify a password equal to the user or equal to the default group.
4. After the addition operation has successfully completed, a panel opens with the new user profile or segment shown with modifiable fields for further customization. The format of this panel is the same as the detail display panel described in "User profile detail display" on page 92.

Application segments

You can use the **Show segments** option or the **SE** action command to view the application segments. For details about each segment and the information provided, select the following links.

CICS segment

The CICS segment stores CICS operator information for a CICS terminal user. Table 48 describes the overview and detail fields included for the segment.

Table 48. CICS segment

Overview field	Detail field	Explanation
Oid	**Operator identification**	Operator identification code
#Cl	n/a	The number of operator classes
Cls	**Operator class**	Operator class value (a number in the range 1 to 24). This value is a repeated field. To see all values, go to the detail display.
Pty	**Operator priority**	Operator priority
TmOut	**Terminal time-out value**	Terminal time-out value (in minutes)
Frc	**XRF Re-signon option**	XRF option for signing back on. This value indicates if CICS signs the operator off after an XRF takeover).
#TK	n/a	Number of Transaction Security Level Keys
#RK	n/a	Number of Resource Security Level Keys
n/a	**Resource SecurityLvl keys**	Resource Security Level Keys
n/a	**Transaction SecurityLvl keys**	Transaction Security Level Keys

CSDATA segment

The `CSDATA` segment stores custom defined profile fields. To add new fields to user profiles, use the `RACF CFIELD` class to define the new fields and labels you want to use for them.

The detail display shows the custom data. The RACF list header is followed by the value formatted according to the type. The value of the custom data is modifiable. Table 49 lists the action commands that can be performed on a custom data entry.

Table 49. CSDATA segment (custom data) action commands

Command	Action
C	Copy custom data. This action opens a panel for specifying the target profile destination for the copied data.
D	Delete custom data.

Table 49. CSDATA segment (custom data) action commands (continued)

Command	Action
I	Insert custom data. This action opens a panel on which you can select an entry name from a list of all defined custom fields. After you select a field, another panel opens on which you can enter the value for the new entry.
R	Recreate custom data. This action generates a RACF command that creates an exact copy of the entry.
S	Select or Modify custom data. This action opens a panel on which you can modify the custom data.

DCE segment

The DCE segment stores DCE (Distributed Computing Environment) info for RACF user IDs. Table 50 describes the overview and detail fields included for the segment.

Table 50. DCE segment

Overview field	Detail field	Explanation
DCE UUID	**DCE UUID**	DCE Universal Unique Identifier
LgA	**DCE Autologin**	Autologon requested.
DCE name	**DCE username**	DCE principal name for the RACF user
DCE homecell	**DCE homecell**	DCE cell for the RACF user
DCE homecell UUID	**DCE homecell UUID**	DCE Universal Unique Ident. in home cell

DFP application segment

The DFP segment stores DFP (Data Facility Product) defaults for RACF user IDs.

Table 51 describes the overview and detail fields included for the segment.

Table 51. DFP segment

Overview field	Detail field	Explanation
MgmtClas	**DFP - Management Class**	The management class
StorClas	**DFP - Storage Class**	The storage class
DataClas	**DFP - Data Class**	The data class
DataAppl	**DFP - Data Application**	The data application

EIM segment

The EIM segment stores Enterprise Identity Manager information for RACF user IDs.

Table 52 describes the overview and detail fields included for the segment.

Table 52. EIM segment

Overview field	Detail field	Explanation
LDAP Profile	**LDAP Profile**	Name of a profile in the LDAPBIND class which contains the name of an EIM domain.

KERB segment

The KERB segment stores Kerberos information for RACF user IDs.

Table 53 describes the overview and detail fields included for the segment.

Table 53. KERB segment

Overview field	Detail field	Explanation
Kerberos name	**Kerberos name**	Kerberos principal name.
MaxTktLife	**Maximum ticket life**	Maximum ticket life for this user in seconds.
Encryption	**Supported encryption types**	Types of encryption that can be used by this user.
EnTp	**Used encryption type**	The encryption type that has been used.
Kfm	**Password is Passphrase**	Indicates whether the password or passphrase was used to generate the Kerberos key.

LANGUAGE segment

The LANGUAGE segment stores the preferred national languages for the user.

Table 54 describes the overview and detail fields included for the segment.

Table 54. LANGUAGE segment

Overview field	Detail field	Explanation
NL1	**User's primary language**	User primary language
NL2	**User's secondary language**	User secondary language

LNOTES segment

The `LNOTES` segment is used to specify z/OS Lotus® Notes® information.

Table 55 describes the overview and detail fields included for the segment.

Table 55. LNOTES segment

Overview field	Detail field	Explanation
Notes short name	n/a	The Lotus Notes for z/OS short user name associated with the RACF `userid`.

NDS segment

The NDS segment specifies Novell Directory Services information.

Table 56 describes the overview and detail fields included for the segment.

Table 56. NDS segment

Overview field	Detail field	Explanation
Uname	**NDS username**	The Novell Directory Services user name associated with the RACF user ID.

NETVIEW segment

The `NETVIEW` segment stores `NETVIEW` operator information.

Table 57 describes the overview and detail fields included for the segment.

Table 57. NETVIEW segment

Overview field	Detail field	Explanation
Console	**Default console name**	Default console name
Rcv	**Receive undelivered messages**	Receive unsolicited messages
Adm	**Admin auth Graphic Mon Fac**	Admin authority for the Netview Graphic Monitor Facility
#Cl	n/a	Number of scope classes
#Dm	n/a	Number of cross-domain authorities
Control	**Scope of control**	Cross-domain logon authority
Cls	**Operator class**	Scope class. Number from 1 to 2040. To see all values, go to the detail display.
Dom.	**Cross-domain authority**	Cross-domain authorities. To see all values, go to the detail display.
Initial command list	**Initial command list**	Initial command to run whenever the operator logs on to `NETVIEW`.

OMVS segment

The OMVS segment stores UNIX System Services information.

Table 58 describes the overview and detail fields included for the segment.

Table 58. OMVS segment

Overview field	Detail field	Explanation
Uid	**UNIX user (uid)**	Numeric UNIX `uid` (0 = root authority). When fields are modifiable (overtypeable), appending the number with an S (*`1001S`*) adds the SHARED command keyword. You can also specify AUTO, which results in addition of the AUTOuID command keyword. The SHARED and AUTOUID command keywords are available in z/OS 1.4 or with APAR OW52135.
Home directory	**UNIX home path**	UNIX account home directory
Initial program	**Initial program**	UNIX account initial program
AS maxsize	**Max. address space size**	Maximum address space region size (bytes)
CPU max	**Maximum CPU time**	Maximum CPU time for process (seconds)
Files	**Max. files open per proc**	Maximum number of open files (3..262,143 (pre-z/OS V1R7) or 524,288 (z/OS V1R7 and up))
MxMemMap	**Max. data space for mapping**	Maximum data space pages memory mapping
Procs	**Max. nr. of active procs**	Maximum number of processes (3..32767)
Thread	**Max. nr. of active threads**	Maximum number of threads (0..100000)
MemLimit	**Maximum non-shared memory**	Maximum number of bytes of non-shared that can be allocated by the user.

Table 58. OMVS segment (continued)

Overview field	Detail field	Explanation
ShMemMax	**Maximum shared memory**	Maximum number of bytes of shared that can be allocated by the user.

OPERPARM

The OPERPARM segment stores extended MCS console information session information.

Table 59 describes the overview and detail fields included for the segment.

Table 59. OPERPARM segment

Overview field	Detail field	Explanation
CmdSys	**System to send commands to**	The name of the system the operator is connected to for command processing
OpAut	**Console authority**	The command authority in effect for the operator.
L	**Command response logging**	Command response logging on hardcopy
M	**Migration id to be assigned**	Migration console ID to be assigned setting
U	**Receive undelivered messages**	'Undeliverable' messages to be received setting
A	**Receive msgs automated by MPF**	Messages marked for automation in MPF are to be received at the console
H	**Receive hardcopy messages**	This field indicates whether the operator receives messages that are directed to hardcopy
I	**Receive messages for ID 0**	This field indicates whether the operator receives messages directed to console ID 0, the internal console.
u	**Receive messages unknown IDs**	This field indicates whether the operator receives messages directed to unknown console IDs
DOM	**Delete operator messages type**	Delete operator message requests to be received setting
Message level	**LEVEL of msgs to be received**	Level of messages to be received
Key	**KEY keyword of D,CONSOLES,KEY**	KEY keyword for D CONSOLES,KEY
Mon	**Events to be monitored**	Events to be monitored
Stor	**STORAGE in MB for msg queuing**	Maximum storage for message queuing (in MB)
Mform	**Message format**	Message format
Altgrp	**Alternate console group**	Alternate console group
Routcde	**ROUTCODEs for msg reception**	Routecode of message to be received
Mscope	**Mscope systems**	Mscope systems. To see all values, go to the detail display.

OVM segment

The OVM segment stores Unix System Services information.

Table 60 describes the overview and detail fields included for the segment.

Table 60. OVM segment

Overview field	Detail field	Explanation
Uid	OpenVM user (uid)	Numeric Unix uid value
Home directory	OpenVM home path	UNIX account home directory
Initial program	Initial program	UNIX account initial program
File system root	UNIX file system root	Path name for the file system root

Proxy segment

The PROXY segment is only valid for the FACILITY and LDAPBIND classes. It is stores LDAP proxy server information.

Table 61 describes the overview and detail fields included for the segment.

Table 61. PROXY segment

Overview field	Detail field	Explanation
LDAP host	**LDAP host**	Host of LDAP server to contact
Bind name	**Bind distinguished name**	Bind information for LDAP server being contacted

TSO segment

The TSO segment stores Time Sharing Option settings.

Table 62 describes the overview and detail fields included for the segment.

Table 62. TSO segment

Overview field	Detail field	Explanation
DfltUnit	**Default unit name**	Default unit name for DASD allocations
DftKB	**Default logon region size (KB)**	Default region size in KB.
MaxKB	**Maximum region size**	Maximum region size in KB.
H	**Default held sysout class**	Default held sysout class
J	**Default job class**	Default job class
M	**Default message class**	Default message class
S	**Default sysout class**	Default sysout class
Destinat	**Destination identifier**	Default destination
ProcName	**Default logon procedure**	Default logon procedure
Acctnum	**Default account number**	Default account number
Opt	**Mail/Notice/Recon/ OID options**	Mail/Notice/REconnect/ OIDcard options

Table 62. TSO segment (continued)

Overview field	Detail field	Explanation
Prf	**Performance group**	Performance group
Prefix	**UPT control block data**	TSO UPT profile settings: TSO dataset prefix
PI?MOWRL	**UPT control block data**	TSO UPT profile settings: *P* Prompt *I* Intercom *?* Pause *M* Msgid *O* Mode *w* Wtpmsg *R* Recovery *L* Varstorage
Data	**Site data TSO user (2 byte)**	TSO user data. This value is carried over from SYS1.UADS–2 bytes printed in hexadecimal.
Command	**Default command**	Default command

WORKATTR segment

The WORKATTR segment specifies user-specific attributes of a unit of work.

Table 63 describes the overview and detail fields included for the segment.

Table 63. WORKATTR segment

Overview field	Detail field	Explanation
Name (workattr)	**User name for SYSOUT**	User name for SYSOUT
Dept	**Department for delivery**	Department for delivery
Building	**Building for delivery**	Building for delivery
Room	**Room for delivery**	Room for delivery
Account	**Account number**	Account number
n/a	**SYSOUT address line 1**	Indicates SYSOUT delivery address line 1.
n/a	**SYSOUT address line 2**	Indicates SYSOUT delivery address line 2.
n/a	**SYSOUT address line 3**	Indicates SYSOUT delivery address line 3.
n/a	**SYSOUT address line 4**	Indicates SYSOUT delivery address line 4.

Print format

To produce a printable report instead of an interactive display, select the *Print format* option. When this option is selected, other print-related option fields are activated. Use *Customize title* to specify a title for the two header lines to be printed on each page in addition to the main report title. If *Background run* is selected together with *Print format*, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared between all RA options

showing it. To send the report through email, select the *Send as email* option. You are prompted to supply the email options. By default the report is shown in a tabular form for improved readability, formatted into 132 columns. Tag *Full page form* if you would rather have more details. Tag *Narrow print* to force it into 79 columns. You can change the sort order of the results by selecting the *Sort differently* option.

If *Sort differently* is selected, a sort order panel opens for each segment type to be shown. Figure 84 shows a sample of the Sort order panel for the base segment.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Sort order
Command ===> ____________________________________________________________
All users
Specify up to 3 fields to act as alternate base segment sort order
Select with 1 or / and optiopnally 2, 3
_ Userid
_ Name
_ Installation data
_ Owner
_ Default group
1 Last logon/connect date
_ Password interval (descending)
_ By audit priority (descending)
```

Figure 84. Segment - Sort order panel

In the sort order panels, you can specify up to three sort keys by entering 1, 2, or 3 in front of the sort criteria. If you want to sort on just one column, it is also possible to use a / instead of 1.

Figure 85 shows an example of wide tabular print output of user profile base segments, sorted by last connect date.

```
zSecure Admin USER overview - complex DINO     12Sep2000  11:47                                                          page    1
All users, sorted by last connect

User     Name                 DfltGrp  Owner    RIRP SOAgC LCX Int LastCon Connect groups           Pri InstData
C##ATST                       C##A     C##BERT  RI           X  30 17Nov95 C##A
C##CUST  Zsecur DEMO ACCOUNT  C##C     C##C     RI           X  30  7Dec95 C##AAPPC C##C C##CDEMO
                                                                          C##CNG C##CXDEL C##GRACF
C##CXGS  GRPSPEC TEST USER    C##CXGRP C##CXGRP R       g    X  30  7Mayr96 C##CXGRP
C##BJN2  JOSEPHINE NASH       C##B     C##B      I           X  30  4Jun96 C##B
C##CX15  TEST USER FOR DELETE C##C     C##C     RI           X  30 30Aug96 C##C C##CXDEL SYSAPPL         FOR PASSWORD HISTORY MANAGE
C##CX05  TEST USER 5          C##C     C##C     RI           X  30 27Nov96 C##C C##CXDEL
C##BAH2  ANGELA HAYES         C##B     C##B     R            X  30 18Feb97 C##B C##BEPRD
C##BCICS Zsecur TEST CICS     C##B     C##B     RI           X  30 29Mar97 C##AAPPC C##B
C##BUI2  BUICK                C##B     C##B      I           X  30 27Jun97 C##B C##BRACF C##TC2E
C##CCW5  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30  9Sep97 C##C C##CDEMO C##CXDEL        WORKSHOP HANDS-ON USER
C##CCW3  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30 11Sep97 C##C C##CDEMO C##CXDEL        WORKSHOP HANDS-ON USER
C##CCW4  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30 11Sep97 C##C C##CDEMO C##CXDEL        WORKSHOP HANDS-ON USER
C##QA018 TRY TO LOG ON        C##QA    C##QA     I           X  31  7Oct97 C##QA
C##QA18  TEST USER            C##QA    C##QA     I           X  50  7Oct97 C##QA
C##CPR1  PAUL RANDALL         C##C     C##C     RI           X  50 18Nov97 C##C C##CDEMO C##CXDEL
C##BGU3  GUS BAKERVILLE       C##C     C##B     RI       C L X  30  2Jan98 C##B C##C C##CXDEL
C##CCW1  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30  2Jan98 C##C C##CDEMO C##CXDEL        WORKSHOP HANDS-ON USER
C##BQAC4                      C##BQA   C##BQA           gC   X  50  8Jan98 C##BQA C##QC4R              SURROGAT USER TO SUBMIT TESTS
C##CCW2  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30  9Jan98 C##C C##CDEMO C##CXDEL        WORKSHOP HANDS-ON USER
C##BJVO  JANE V ONOTOP        C##B     C##B      I           X  90 20Mar98 C##B C##PC2E C##TC2E
C##BDMW  DAN WIGHT            C##B     C##B      I           X  30 26Mar98 C##B
C##BJM1  JEROEN MAN           C##B     C##B      I           X  90  3Apr98 C##B C##PC2E C##TC2E
C##BJNG  JOSEPH NGAI          C##B     C##B      I           X  30 10Jun98 C##B
C##CHAI  DENNIS HAILEY        C##C     C##C     RI           X  90 12Jun98 C##C C##CXDEL
C##QA050                      C##QA    C##QA     I P       L      18Jun98 C##QA                       QR61113 TESTSUBJECT
C##QAP0  TEST RUNNER1         C##QA    C##QA     I     g           2Jul98 C##ARACF C##BREAD C##CNG
```

Figure 85. User overview report

For the meaning of the columns see “User profile tabular display” on page 89.

When *Narrow print* is checked, the results are shown with connects and installation data on a separate line:

```
RACF userids   - complex DINO     12Sep2000  12:19                  page    1
All users, sorted by last connect

User     Name                DfltGrp  Owner    RIRP SOAgC LCX Int LastCon Pri
C##ATST                      C##A     C##BERT  RI           X  30 17Nov95
         Connects: C##A
C##CUST  Zsecur DEMO ACCOUNT  C##C     C##C     RI           X  30  7Dec95
         Connects: C##AAPPC C##C C##CDEMO C##CNG C##CXDEL C##GRACF
C##CXGS  GRPSPEC TEST USER    C##CXGRP C##CXGRP R       g    X  30  7Mar96
         Connects: C##CXGRP
C##BJN2  JOSEPHINE NASH       C##B     C##B      I           X  30  4Jun96
         Connects: C##B
C##CX15  TEST USER FOR DELETE C##C     C##C     RI           X  30 30Aug96
         Connects: C##C C##CXDEL SYSAPPL
         Data: FOR PASSWORD HISTORY MANAGED BY CKGRACF
C##CX05  TEST USER 5          C##C     C##C     RI           X  30 27Nov96
         Connects: C##C C##CXDEL
C##BAH2  ANGELA HAYES         C##B     C##B     R            X  30 18Feb97
         Connects: C##B C##BEPRD
C##BCICS Zsecur TEST CICS     C##B     C##B     RI           X  30 29Mar97
         Connects: C##AAPPC C##B
C##BU12  BUICK                C##B     C##B      I           X  30 27Jun97
         Connects: C##B C##BRACF C##TC2E
C##CCW5  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30  9Sep97
         Connects: C##C C##CDEMO C##CXDEL
         Data: WORKSHOP HANDS-ON USER
C##CCW3  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30 11Sep97
         Connects: C##C C##CDEMO C##CXDEL
         Data: WORKSHOP HANDS-ON USER
C##CCW4  Zsecur/CCW + VIEW    C##C     C##C     RI           X  30 11Sep97
         Connects: C##C C##CDEMO C##CXDEL
         Data: WORKSHOP HANDS-ON USER
C##QA018 TRY TO LOG ON        C##QA    C##QA     I           X  31  7Oct97
         Connects: C##QA
C##QA18  TEST USER            C##QA    C##QA     I           X  50  7Oct97
         Connects: C##QA
C##CPR1  PAUL RANDALL         C##C     C##C     RI           X  50 18Nov97
         Connects: C##C C##CDEMO C##CXDEL
```

For the meaning of the columns see "User profile tabular display" on page 89.

When *Full page form* is selected in combination with *Show segments* and *All*, a full, page-wide print report like the following is created.

```
RACF userid C##BGRA  GERTIE RANDALL       complex DINO     12Sep2000  13:59        page    1
Users like C##BGRA

Identification
--------------
RACF userid                   C##BGRA
User name                     GERTIE RANDALL
Owner                         C##B                        EMPLOYEES
User's default group          C##B                        EMPLOYEES

Connects Auth    R SOA AG Uacc    Revokedt    Resumedt    InstData
-------- ----    -------- ----    --------    --------    --------
C##B     USE             NONE                            EMPLOYEES
C##BDOC  USE             NONE                            UPDATE/MAINTAIN (NEW) ONLINE BOOKS

System access                        Statistics                            Privileges
-------------                        ----------                            ----------
Revoked (may be by date)      Yes    Creation date                03Mar1998 Security admin    SPECIAL on
Inactive, revoked or pending  Yes    Last RACINIT current connects 28Aug2002 DASD administrator OPERATION No
Days of week user can logon   SMTWTFS User's last use date         28Aug2002 Global audit set/list AUDITOR No
Time of day user can logon             User's last use time       13:54:28  Class authority
Date user will be revoked
Date user will be resumed

Password                              Password phrase                 Safeguards
--------                              ---------------                 ----------
Has a password                Yes     Has a password phrase        No Ignore UACC/Glob/* RESTRICTED No
Expired password              No      Expired password phrase      No Log all user actions   UAUDIT No
Password changed date         15Mar2006 Password phrase change date
Password expiration date      13Aug2006 Password phrase expiry date
Old passwords present #        25     Old pass phrases present #    0
Failed password attempts #      0
Password interval              90     Mandatory Access Control
Password interval in effect    90     -------------------------
Mixed case password           Yes     Security label
Has a password envelope               Security level
Password disabled   PROTECTED No      Categories list

Safeguards
----------
Ignore UACC/Glob/* RESTRICTED No
Log all user actions   UAUDIT

TSO output settings                   TSO limitations                TSO last logon settings
-------------------                   ---------------                -----------------------
Default message class         A       Maximum region size      16000 Default logon region size(KB)8000
Default sysout class                  Default unit name              Default logon procedure      TSOPROC2
Default held sysout class             Site data TSO user (2 byte)0000 Default account number
Default job class                                                    Default command              INIT#FB
```

```
Destination identifier                                  Performance group              0
                                                        Mail/Notice/Recon/OID options MNR
                                                        UPT control block data       C##BGRA PW
```

When *Narrow print* is also selected, a print file like the following results:

```
C##BGRA  GERTIE RANDALL        DINO     12Sep2000  14:07 BASE          page    1
Users like C##BGRA

Identification
--------------
RACF userid                   C##BGRA
User name                     GERTIE RANDALL
Owner                         C##B                          EMPLOYEES
User's default group          C##B                          EMPLOYEES

Connects Auth    R SOA AG Uacc    Revokedt    Resumedt    InstData
-------- ----    -------- ----    --------    --------    --------
C##B     USE              NONE                            EMPLOYEES
C##BDOC  USE              NONE                            UPDATE/MAINTAIN (NEW)

System access                           Statistics
-------------                           ----------
Revoked (may be by date)      Yes       Creation date                 03Mar1998
Inactive, revoked or pending  Yes       Last RACINIT current connects 28Aug2002
Days of week user can logon   SMTWTFS   User's last use date          28Aug2002
Time of day user can logon              User's last use time          13:54
Date user will be revoked
Date user will be resumed

Password                                Password phrase
--------                                ---------------
Has a password                Yes       Has a password phrase         No
Expired password              No        Expired password phrase       No
Password changed date         15Mar2006 Password phrase change date
Password expiration date      13Aug2006 Password phrase expiry date
Old passwords present #        25       Old pass phrases present #      0
Failed password attempts #      0
Password interval              90
Password interval in effect    90
Mixed case password           Yes
Has a password envelope
Password disabled   PROTECTED No

Mandatory Access Control                                  Privileges
------------------------                                  ----------
Security label                ........  Security admin        SPECIAL No
Security level                          DASD administrator    OPERATIONS No
                                        Global audit set/list AUDITOR No

Safeguards
----------
Ignore UACC/Glob/* RESTRICTED No
Log all user actions   UAUDIT No

TSO output settings                     TSO limitations
-------------------                     ---------------
Default message class         A         Maximum region size          16000
Default sysout class                    Default unit name
Default held sysout class               Site data TSO user (2 byte)   0000

TSO last logon settings
-----------------------
Default logon region size(KB) 8000
Default logon procedure       TSOPROC2
Default account number
Default command               INIT#FB
Performance group               0
Mail/Notice/Recon/OID options MNR
UPT control block data        C##BGRA P    W
```

RA.G GROUP - Group information

The Group information panel provides access to simple selection functions for groups. Using these functions, you can do things like the following:

- Add a new group or segment. See "Add new group or segment" on page 127.
- Specify selection criteria for GROUP profiles.

Only profiles that match **all** criteria are selected. In effect, all the search criteria are combined with AND logic.

The simple selection panel is shown in Figure 86 on page 118.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Selection
Command ===> ____________________________________________   _  start panel

_   Add new group or segment

Show groups that fit all of the following criteria
Group id  . . . . . ________     (group profile key or filter)
Owner . . . . . . . ________     (group or userid, or filter)
Subgroup of . . . . C##B____     (group or filter)
With subgroup . . . ________     (group or filter)
Installation data . ____________________________ (data scan, no filter except *)

Additional selection criteria
_  Profile fields     _  Connect fields   _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Expand universal  _  Specify scope
_  Print format       _  Customize title  _  Send as email

   _  Background run  _  Full detail form _  Sort differently  _  Narrow print
   _  Print connects  _  Print names      _  Print subgroups
```

Figure 86. Simple group selection

The following selection criteria are available.

Table 64. Group selection criteria

Criteria	Description
Group Id	This group ID, or a matching ID if a filter is used.
Owner	If specified, groups are selected based on the OWNER value you specify. The owner can be a user or group. It is possible to use a filter.
Subgroup of	You can select an entity through its superior group. It is possible to use a filter to select an entity through more than one superior group.
With subgroup	You can select an entity through its subgroups. The select group is the superior group of the group you specify here. It is possible to use a filter to select an entity through more than one subgroup.
Installation Data	Data to scan for in the installation data field. You cannot use a filter except *, which means find any profile with installation data.

Additional selection criteria can be requested by selecting the following options.

Table 65. Additional Group selection criteria

Criteria	Description
Profile fields	When you select this option, another panel opens for selecting criteria based on profile field values. The selection panel is shown in "Additional selection - Profile fields" on page 120. If the field is not selected, the **Profile fields** selection criteria are not used but are saved for later use when you remain in **RA.G**.
Connect fields	Use this option to specify criteria to select based on d users. The selection panel is shown in "Additional selection - Connect fields" on page 121. If the field is not selected, those selection criteria are not used but are saved for later use when you remain in **RA.G**.

Table 65. Additional Group selection criteria (continued)

Criteria	Description
Segment presence	If this field is selected, criteria can be specified for the presence of application segments. A segment selection panel and a segment field selection panel are shown. Unless the output option **Show segments** has also been selected, these panels only show the base segment of groups that have the specific non-base segment. If the field is not selected, the selection criteria are not used but are saved for later use when you remain in **RA.G**.
Segment absence	If this field is selected, absence of a segment can be specified as an additional selection criterion. If the field is not selected, the selection criteria are not used, but are saved for later use when you remain in **RA.G**.

Table 66 lists the output and run options you can specify.

Table 66. Output and run options for Groups

Option	Description
Show segments	Show a selectable set of application segments for specifying select and exclude criteria based on segment field values. If this option is not selected, the segment subset is not used but is saved in your ISPF profile for later use. This flag setting is saved in your ISPF profile.
All	Select this option with *Show segments* to show all segments for the selected groups.
Expand universal	Select this option to request that the default connections to universal groups are shown for profiles with connect authority `USE` and no group special, operations, or auditor attribute. This setting implies a full database read. If **Print format** is also specified, the **Expand universal** option only has effect when **Print connects** is also specified or implied.
Specify scope	If this field is selected, you can limit the results to the scope of a user ID or group.
Print format	If this field is selected, results are in print format instead of ISPF display format. This flag setting is saved in your ISPF profile and is shared between all **RA** options showing it. The other print-related options only apply if **Print format** has been selected. See also “Print format” on page 129.
Customize title	If this field is selected together with **Print format**, you can change the subtitle for the selection. You can also add an extra title that is saved in your ISPF profile, including your company name, department, and phone number for example. This flag setting is saved in your ISPF profile and is shared among all **RA** options that include this field.
Send as email	If this field is selected along with **Print format**, then a panel opens for specifying the email address destination for the report. The email function does not work until you have configured the SMTP options with `SETUP OUTPUT`. This flag setting is saved in your ISPF profile and is shared by all **RA** options showing it.
Background run	If this field is selected together with **Print format**, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared by all `RA` options showing it.

Table 66. Output and run options for Groups (continued)

Option	Description
Full detail form	If this field is selected together with **Print format**, forms (one subpage per group, separated by dashed lines) are used to include details. This selection implies selections for the **Print connects**, **Print names**, and **Print subgroups** options. This flag setting is saved in your ISPF profile. If you have requested segments, they are shown on the same page with the other group information. If the **Full detail form** field is not selected, each segment type is shown in its own tabular report. Sample output is shown in "Print format" on page 129.
Sort differently	If this field is selected together with **Print format**, then an alternate sort order can be selected. If you want to change the sort order in an ISPF display panel (**Print format** not selected), you can use the `SORT` primary command in the result panel. This flag setting is saved in your ISPF profile.
Narrow print	If this field is selected together with **Print format**, then the width of the page is limited to 79 characters, independent of the actual print file record length. If the field is not selected, then the page layout you specify must support a width of 132. However, the length can extend beyond that if the print file has a larger record length. This flag setting is saved in your ISPF profile and is shared by all panels showing this option.
Print connects	If this field is selected with **Print format**, then the connect entries are printed. The `Exact` format depends on the **Print names** and **Narrow print** settings. The default sort order (by descending access) can be changed by checking the **Sort differently** option. The **Print connects** option is automatically implied by **Full detail form**. If you want to limit the number of lines in the results, do not select the **Print connects** option. This flag setting is saved in your ISPF profile.
Print names	If this field is selected with the **Print format** and **Print connects**, then the connect entries are printed with names and installation data added. Only the first part of the installation data is printed, depending on the setting of option **Narrow print**. If **Narrow print** is selected, then the revoke and resume dates for connect entries are not visible in the report. This flag is implied by **Full detail form**. This flag setting is saved in your ISPF profile.
Print subgroups	If this field is selected with the **Print format** and **Print connects**, then the subgroups are listed. This flag setting is saved in your ISPF profile.

Additional selection - Profile fields

In the example shown in Figure 86 on page 118, the subgroups of *C##B* have been selected. If the option **Profile fields** has also been checked, the advanced selection panel shown in Figure 87 on page 121 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Selection
Command ===> ____________________________________________________________

Subgroups of C##B
Show groups that also fit all of the following criteria:
Selection by date
Creation date . . . __   ___________          (date: yyyy-mm-dd/ddMMMyyyy/
                                                    DUMPDATE/DUMPDATE-nnn/
                                                    TODAY/TODAY-nn/NEVER)

Miscellaneous fields
Complex . . . . . ________     (complex name or filter)
# connected users . >_  2___                 (operator: < <= > >= = <> ¬= )
# subgroups . . . . __  ____

Enter "/" to specify selection criteria
_  Universal group
_  Queued commands
_  Userdata
```

Figure 87. Advanced group selection

In this second panel, an additional selection criteria is specified to select only groups that have more than two connected users.

The following additional selection criteria are available on this panel:

Table 67. Additional group selection criteria

Criteria	Description
Creation date	Test the day the group was defined to RACF
Complex	In a complex with this name, or a matching complex if a filter is used.
# connected users	Test the number of connected users, with comparison operators. For universal groups, this number only includes the users with non-default connections. That is, users with a connect authority higher than USE or users with the group attributes `SPECIAL`, `OPERATIONS`, or `AUDITOR`.
# subgroups	Test the number of subgroups, with comparison operators.
Universal group	Show only groups with the UNIVERSAL attribute.
Queued commands	Show only groups with one or more commands queued.
Userdata	Show only groups with `userdata`.

Additional selection - Connect fields

In the example shown in Figure 86 on page 118, the subgroups of C##B that have more than two users have been selected. You can use **Connect fields** for specifying additional selection criteria based on Connect field values. When you select this option, the advanced selection panel shown in Figure 88 on page 122 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Selection
Command ===> ____________________________________________________________________
Subgroups of C##B, #connects>2

Specify additional group selection criteria
Connected user  . . ________ (userid or filter)

Connect authority . __    _   1. Use   2. Create   3. Connect  4. Join


Specify output filtering for the list of connects
User/authority  . .       _  Match selection above

Default UACC  . . . >_    _  1. None  2. Read  3. Update  4. Control  5. Alter

Set of attributes . OR_   _  Special       _  Operations    _  Auditor
                          _  Revoked
```

Figure 88. Group connect selection

Table 68 describes the following additional selection criteria on this panel:

Table 68. Group connection selection criteria

Criteria	Description
Connected user	Search for groups with the specified user ID on the connect list.
Connect authority	Test for the following connect authorities using comparison operators: `USE`, `CREATE`, `CONNECT`, or `JOIN` authority.

When performing these selections against groups with the `UNIVERSAL` attribute, the only connects considered are for groups that have either a connect authority higher than `USE` or the group attributes `SPECIAL`, `OPERATIONS`, or `AUDITOR`.

Table 69 describes the filtering options available on the Group Connection panel.

Table 69. Group connection output filtering options

Option	Description
User/authority Match selection above	You can limit the number of connects shown with a group to the ones that match the **Connected user** and **Connect authority** search criteria.
Default UACC	You can limit the number of connects being shown with a group to the ones that satisfy the comparison operator applied to the default universal access. The default UACC is only used when the user creates a profile in a class that has the ACEE setting as the default UACC. See the “STATUS AUDIT - RACF control” on page 266 CDT option.
Set of attributes	Use the operator to determine how the authorities relate to each other. Specify `OR` or `AND` to filter using combined attributes.
Special	Selects all connects that have Group Special authority. User IDs that have this authority can change, delete, and create any group-owned profile for a specific group.
Operations	Selects all connects that have Group Operations authority. User IDs that have this authority can alter group-owned data sets unless they are specifically on the access list.
Auditor	Selects all connects that have Group Audit authority.

Table 69. Group connection output filtering options (continued)

Option	Description
Revoked	Selects all Connects that are currently revoked, which includes the Connects that were revoked at the *dumpdate* for the security database. This value selects connect entries based on the values of the `revoke flag`, `revoke date`, and `resume date`.

Group profile tabular display

As a result of a query, a group list can be produced like the one shown in Figure 89. Fields that can be modified are shown padded with underline characters.

```
zSecure Admin Group Overview                                  Line 1 of 8
Command ===> ____________________________________________________ Scroll===> CSR
Subgroups of C##B with #connects>2              12 Sep 2000 17:41
   Group    Complex  SupGroup X Owner     Grps   Users  Conn U nTU Created
__ C##BDOC  TODAY    C##B____   C##B____              5     5   ___ 21Oct1996
__ C##BEPRD TODAY    C##B____   C##B____              9     9   ___ 01Mar1997
__ C##BMR   DINO     C##B____ X C##BMR2_              4     4   ___ 17Apr2000
__ C##BOMVS TODAY    C##B____   C##B____              3     3 U ___ 18Feb1998
__ C##BQA   TODAY    C##B____   C##B____              6     6   YES 18Jul1996
__ C##BREAD TODAY    C##B____   C##B____             49    49   ___ 14Nov1995
s_ C##BSUPP TODAY    C##B____   C##B____      1       3     3   ___ 08Dec1997
__ C##BTSUP TODAY    C##B____   C##B____              7     7   ___ 03Apr1998
********************************** BOTTOM OF DATA ***************************
```

Figure 89. Group profile display

Table 70 describes the fields of interest on the Group Profile display panel.

Table 70. Group profile display important fields

Field	Description
Group	The name of the group.
Complex	The name of the complex.
SupGroup	The superior group.
X	Indicates an interruption in group ownership. A break occurs if the owner and superior group differ.
Owner	The owning user or group for a group profile.
Grps	The number of subgroups that have this group as superior group
Users	The total number of users connected to this group, even for `UNIVERSAL` groups.
Conn	The number of users connected to this group. For a group with the universal attribute, this field only counts users that have a group access level higher than the default level.
U	If a U is shown in this column, the group has the `UNIVERSAL` attribute.
nTU	For all connected users: no terminal access based on `UACC`.
Created	Creation date of this group
Pri	The relative audit priority for this group.
InstData	Installation data

Group profile detail display

Select any group on the group profile table display to see the detail view. You can select entries by putting the cursor on the first character of a row selection field and pressing **Enter**, or by explicitly typing S and pressing **Enter**.

```
zSecure Admin Group Overview                                  Line 1 of 29
Command ===>                                                    Scroll===> CSR
 Subgroups of C##B with #connects>2            26 Jan 1999 00:05


  Identification                                                       DINO
_ RACF group name              C##BSUPP
_ Superior group               C##B____ EMPLOYEES
_ Owner                        C##B____                    EMPLOYEES
  Installation data            CUSTOMER SUPPORT_____________________________

  User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt    Name
_ C##BNA1_ USE____ _ ___ __ NONE___ ___________ ___________ NATHAN ADRIAN
_ C##BWTK_ USE____ _ ___ __ NONE___ ___________ ___________ WILLIAM KATZ
_ C##BWT2_ USE____ _ ___ __ NONE___ ___________ ___________ WILLIAM KATZ 2
_ C##CHPM_ USE____ _ ___ __ NONE___ ___________ ___________ HENRY PEMBROKE

  SubGroup InstData
_ C##CDEMO FOR DEMONSTRATION USERIDS

  Safeguards                           Statistics
  Terminal use authorization   No_     Creation date                8Dec97
  Universal access authority   NONE     Universal group              No
  Data set model profile name  ____________________________________________

  Timed commands waiting for execution
_ Queued command (P): CMD AT 03Oct2000 UNTIL 04Oct2000 REMOVE   C##QA022 GRO(CR
******************************* BOTTOM OF DATA ********************************
```

Figure 90. Group Profile detail display

The fields shown on the Group Profile detail display panel depend on the SETUP configuration and data availability.

Identification fields. Table 71 describes the Identification fields.

Table 71. Group profile detail display - Identification fields

Field	Description
Identification	To the far right, the complex name is shown.
RACF group name	The RACF profile key.
Superior group	Lists the parent group for this group in the group tree followed by its installation data.
Owner	The owning user or group followed by the user name and the user or group installation data.
Installation data	Installation data field of the group.

Connect fields. Table 72 on page 125 describes these fields. If the current group has the UNIVERSAL attribute, you can control whether users with default connect attributes are shown by issuing the ACL UNIVERSAL and ACL NOUNIVERSAL primary commands.

Table 72. Group Profile detail display - Connect fields

Field	Description
User/grp	Users connected to the group
Auth	Connect authority
R	Indicates whether this connect is revoked. This setting is determined by considering any revoke and resume dates and the database `dumpdate`.
SOA	Indicates whether the user has the following group attributes: `SPECIAL`, `OPERATIONS`, or `AUDITOR`.
AG	Settings used for new data set or resource profiles created while the user is logged on with this group as the current connect group. The *A* for ADSP is only used if the system-wide SETROPTS ADSP option has also been set. It controls whether creation of a data set automatically results in creation of a discrete data set profile. Its use is deprecated. The G for `GRPACC` regulates whether the group must be added with UPDATE access to new group data set profiles
Uacc	Default universal access for new data set or resource profiles created while the user is logged on with this group as the current connect group.
Revokedt	Revoke date of connect
Resumedt	Resume date of connect
Name	Name of connected user
DfltGrp	Default group for the user
InstData	Installation data field of the user

Subgroup fields. Table 73 describes these fields.

Table 73. Group Profile detail display - Subgroup fields

Field	Description
Subgroup	The groups for which this group is the superior group
InstData	Installation data field of the subgroup

Safeguard fields. Table 74 describes these fields.

Table 74. Group Profile detail display - Safeguard fields

Field	Description
Terminal use authorization	Indicates whether Terminal use authorization is required for all connected users. If this option is selected, terminal access is not granted based on UACC.
Universal access authority	The default Universal Access Authority for the group profile.
Data set model profile name	Name of a discrete data set profile for modeling new `group-name` data sets.

Statistics fields. Table 75 on page 126 describes these fields.

Table 75. Group Profile detail display - Statistic fields

Field	Description
Creation date	The date that the profile was created.
Universal group	Whether this group has the UNIVERSAL attribute. With this attribute, there is no limit on the number of users that can connect to a group with default authorities.

Additional, optional properties. Table 76 describes these fields.

Table 76. Group Profile detail display - Additional, optional properties fields

Field	Description
Audit concern	A concatenation of audit concerns for the group.
UsrNm	The names of the `userdata` fields, excluding the fields used by `CKGRACF`.
Flg	Flag associated with the `userdata` field
UserData	Contents of the `userdata` field
CKGRACF authority requirement	Authority required to change this GROUP profile. Possible values are: SINGLE, DOUBLE or TRIPLE. These values represent the number of administrators who must sanction a command.
Timed commands waiting for execution	`P` indicates time commands that have been approved and are now waiting for the scheduled run date. `PR` indicates temporary commands that remain in this queue waiting for their reversal date.
Commands requiring administrator action	Commands that have not been fully authorized yet as per the value specified in the **CKGRACF authority requirement** field or based on the system-wide default value.
Inactive commands	Requested commands that were not fully authorized and then expired, were withdrawn, or were denied. These commands are included in the audit trail with others that were not run.
Commands that have been executed	Commands that were fully authorized and run. These commands are included in the audit trial.

For an explanation of the CKGRACF data, see "RA.2 QUEUED - Queued commands" on page 185 and "MR - CKGRACF mulitple authority requirement" on page 63.

Line commands for a group profile display

When you use **/** line command to ask which line commands are permitted, the following table is shown.

Table 77. Group profile display - Line commands

Command	Meaning	Explanation
A	Group authorization (permits and scope)	"RA.3.4 Permit/Scope - Report access of a user or group" on page 207
AC	Access check for group on one profile	"RA.1 ACCESS - Access Check" on page 184
C	Copy group ID.	"C - Copy" on page 55
CO	Add connect.	"CO - Add connect" on page 57

Table 77. Group profile display - Line commands (continued)

Command	Meaning	Explanation
D **DD**	Delete group, or delete a non-base segment	"D - Delete" on page 58
E	Display event logging.	"E - Event" on page 59
L	RACF `listgrp` all command	The results of the `listgrp` command is presented in a browse panel.
MI	Manage group information.	"MI - Manage information" on page 61
MR	Manage `CKGRACF` authority requirements	"MR - CKGRACF mulitple authority requirement" on page 63
MU	Manage installation-defined `userdata`	"RA.3.9 USERDATA - User data management" on page 219
PE	Add or delete permit	"PE - Add or delete permit" on page 69
R **RR**	Recreate group ID	"R - Recreate a profile" on page 70
S	Show additional information	"S - Select" on page 72
SE	Show application segments	"SE - Show application segments" on page 72 and "Application segments" on page 128.
SR	Show all relevant information	"SR - Show all Relevant information" on page 73
X **XX**	Exclude group ID from `FORALL` processing.	"X - Exclude profile line command" on page 74
Z **ZZ**	Select group ID for `FORALL` processing.	"Z - Select a profile" on page 74
34	Data Set List Utility	"34 - Data set list utility" on page 74

Add new group or segment

You can add a new group or segment to the current system with the **Add new group or segment** option on the RACF Group Selection panel (Figure 86 on page 118).

You can also add a new profile by copying an existing one. For details, see "C - Copy" on page 55. If you want to add a group or segment on another system, you must use a batch job.

Use the following procedure to add a new group or segment from the RACF Group Selection panel.

1. On the RACF Group Selection panel (Figure 86 on page 118), type a / or *S* in the **Add new group or segment** field.
2. Press **Enter** to open the Add GROUP panel.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Add
Command ===> ____________________________________________________________

Group id  . . . . . ________     (required)
Superior group  . . C##C____     (required for define new profile)
Owner . . . . . . . =________    (userid, or better = to use superior group)

/   Define new GROUP profile              _  Universal group
_   Add CSDATA segment
_   Add DFP segment
_   Add OMVS segment
_   Add OVM segment
_   Add TME segment
```

Figure 91. ADD GROUP panel

3. On the Add panel, you can add a new group, add a segment to an existing group, or add a combination of a group and segment. For information on performing these tasks, see the ISPF panel help.
4. After specifying the field information, press **Enter** to the immediately add the group or segment on the system you are logged on to.

   The RACF command response is only shown if there is a nonzero return code.

Notes:

1. When the Add panel displays, the default superior group and owner are stored in your ISPF profile based on previous add group operations. This information is provided to support users that do most of their additions in the same group.
2. After the addition operation has successfully completed, a panel opens with the new profile or segments shown with modifiable fields for further customization. The format of this panel is the same as the detail display panel described in "Group profile detail display" on page 124.

Application segments

When the **Show segments** option is selected, or the **SE** action command is used, application segments are displayed.

The CSDATA segment stores custom defined profile fields. To add new fields to group profiles, use the RACF `CFIELD` class to define the new fields and labels you want to use for them.

The detail display shows the custom data; the RACF list header followed by the value formatted according to the type. The value of the custom data is modifiable. Table 78 lists the action commands that can be performed on a custom data entry.

Table 78. CSDATA segment (custom data) action commands

Command	Action
C	Copy custom data. This action opens a panel for specifying the target profile where the data is copied.
D	Delete custom data.
I	Insert custom data. This action opens a panel on which you can select an entry name from a list of all defined custom fields. After you select a field, another panel opens on which you can enter the value for the new entry.

Table 78. CSDATA segment (custom data) action commands (continued)

Command	Action
R	Recreate custom data. This action generates a RACF command that creates an exact copy of the entry.
S	Select/Modify custom data. This action opens a panel on which you can modify the custom data.

The DFP segment is used to store DFP (Data Facility Product) defaults for RACF groups.

Table 79. DFP segment

Field	Explanation
MgmtClas	The management class
StorClas	The storage class
DataClas	The data class
DataAppl	The data application

The group OMVS segment display shows the group ID for the UNIX System Services. When the `Overtype` function is active, you can append an *S* to the number (*1001S*) to add the `SHARED` command keyword. You can also specify AUTO, which results in addition of the `AUTOGID` command keyword. The `SHARED` and `AUTOGID` command keywords are available in z/OS 1.4 or with APAR OW52135.

The group OVM segment display shows the group ID for z/VM OpenExtensions.

The group TME segment detail display lists the role access specifications for the group in the Tivoli Management Environment. The segment display shows the number of specifications and the first specification.

Print format

To produce a printable report instead of an interactive display, select the **Print format** option. When you select this option, the other print-related options are available for selection. Select **Customize title** to specify two header lines to be printed on each page in addition to the main report title. To send the report through email, select the **Send as email** option. You are prompted to supply the email options. By default the report is shown in a tabular form for improved readability, formatted into 132 columns. Tag **Full page form** if you would rather have more details. Tag **Narrow print** to limit the page width to 79 columns. You can change the sort order of the results by selecting the **Sort differently** option. When you select this option, a sort order panel is shown for each segment type to be included in the report. Figure 92 on page 130 shows the sort panel for the base segment:

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Sort Order
Command ===> ____________________________________________________________
All profiles
Specify up to 3 fields to act as
alternate base segment sort order
Select with 1 or / and optionally 2, 3
_ Group name (default)
_ Grouptree traversal
_ Depth
_ Installation data
_ Owner
_ Superior group
_ Break in group scope
_ Number of groups (descending)
_ Number of users (descending)
_ Creation date (descending)
_ Terminal universal access
_ Universal access (descending)
_ By audit priority (descending)
```

Figure 92. Group sort order panel

In the sort order panels, you can specify up to three sort keys by entering *1*, *2*, or *3* in front of the sort criteria. If you want to sort on just one column, it is also possible to use a / instead of *1*.

Figure 93 shows an example report with wide tabular print format of group profile base segments, sorted by descending number of users.

```
zSecure Admin Group Overview - complex DINO     12Sep2000  15:14                                                    page    1
All profiles, sorted by users

Group    Lvl SupGroup X Owner     Grps Users  Conn Uni nTU Created   Pri InstData
C##QA      5 C##Q       C##Q         7   231   231     nTU 18Jul1996     C## Q.A. TESTSUBJECT
C##C       3 C#         C#           6   218   218         07Nov1995     EXTERNAL USERS
C##CXDEL   5 C##CXCNG   C##CXCNG     2   214   214         16Feb2000     TEST GROUP FOR DEVELOPMENT
C##B       3 C#         C#          13    87    87     nTU 14Nov1995     EMPLOYEES
REVOKE     3 SYSAUTH    SYSAUTH          80    80         24Feb2000
C##GRACF   3 C#         C#               42    42         07Nov1995     PADS LIVE RACF+SMF
C##BREAD   4 C##B       C##B             39    39         14Nov1995     READ SOURCE
C##CNG     4 C##        C##              32    32         07Nov1995     USE CKGRACF FUNCTIONS ON C#
C##BRACF   4 C##A       C##A             20    20         14Nov1995     DIRECT LIVE RACF+SMF+PADS
C##A       3 C#       X C##AINT      8   17    17         04Nov1995     MANAGEMENT
C##ARACF   4 C##A       C##A             15    15         14Nov1995     DIRECT LIVE RACF+SMF
C##BEPRD   4 C##B       C##B             14    14         01Mar1997     EPRISE DEVELOPMENT
C##BQAMC   6 C##QA      C##QA            14    14     nTU 01Nov1996     CNGTEST
OMVSGRP    4 SYSAPPL    SYSAPPL          13    13         23Jan1996
C2RADMIN   3 SYSAUTH    SYSAUTH          12    12         27Feb1999     RACFWIN-SERVER ADMINISTRATO
```

Figure 93. Group profile base segments report in wide tabular print format

For the meaning of the columns see "Group profile tabular display" on page 123.

When **Narrow print** is selected, the report format is almost the same. If **Print connects** and **Print subgroups** are also selected, this format changes to show subgroups and connects on a separate line as shown in Figure 94 on page 131.

```
RACF GROUP profiles  - complex DINO     12Sep2000  16:45              page    1
All profiles

Group    Lvl SupGroup XTU Owner     Grps Users  Conn Created Pri InstData
ADMIN      3 SYSUSER      SYSUSER            4     4 16Mar97     GRP =QA CNG SC
    Users:      ADM1      ADM2     FIN1     FIN2
AJV        3 SYSAUTH      SYSAUTH                     25Jul98     JAVA FOR OS390
ANF        3 SYSAUTH      SYSAUTH                     17Feb98     IP PRINTWAY
API        3 SYSAUTH      SYSAUTH                     17Feb98     NETSPOOL
APPL       3 SYSUSER      SYSUSER                     16Mar97     GRP =QA CNG SC
ASM        3 SYSAUTH      SYSAUTH                     26Apr99     HLASM + TOOLKI
ASMA       3 SYSAUTH      SYSAUTH                     17Feb98     HLASM
ASMT       3 SYSAUTH      SYSAUTH                     17Feb98     HLASM TK
ASPSERV    3 SYSAUTH      SYSAUTH                     18Feb98
ASU        3 SYSAUTH      SYSAUTH                     17Feb98     DCE
AUD1       3 SYSUSER  X   AUDIT              3     3 16Mar97     GRP =QA CNG SC
    Users:      AUD2      AUD2X    AUD3
BCP        4 SYSPROG      SYSPROG                      7Nov95
BDT1       3 SYSAUTH      SYSAUTH                     18Feb98
BFS        3 SYSAUTH      SYSAUTH                     17Feb98     LAN SERVER
BOOKS      2 SYS1         SYS1                        15Feb97
CATALOG    4 SYSPROG      SYSPROG                      7Nov95     ICF CATALOGS
CBC        4 SYSPROG      SYSPROG                      7Nov95     C/C++
CBCV1R3    3 SYSAUTH      SYSAUTH                     11Jan99     C CLASS LIBRAR
CDS        3 SYSAUTH      SYSAUTH                     27Apr99     OCSF
CEE        3 SYSAUTH      SYSAUTH                     17Feb98     LE
CEEV1R3    3 SYSAUTH      SYSAUTH                     11Jan99     LE DATASETS
CMX        3 SYSAUTH      SYSAUTH                     26Apr99     HCM
CNM        3 SYSAUTH      SYSAUTH                     26Apr98     NETVIEW
CPAC       3 SYSAUTH      SYSAUTH                     17Feb98     CUSTOM PACK DA
C#         2 SYS1         SYS1         7     1     1  4Nov95
    Subgroups:  C#ADMIN C## C##A C##B C##C C##GRACF C2R
    Users:      C##QA020
C#ADMIN    3 C#           C#                 11    11 28Apr98     SYSTEM ADMIN E
                                                                   ENCY USER ADMI
    Users:      AUTO1     AUTO2    CNMCSSIR CNM01PPT C##BERT  C##BMB1  C##BMB2
    Users:      C##BPK1   C##BPK2  RCCSL01
C##        3 C#           C#            8     2      2  7Nov95     DATA SETS FOR
                                                                  ALL TEST
    Subgroups:  C##CNG C##PC2E C##PC4R C##Q C##QC4R C##TC2A C##TC2E C##TC4R
    Create:     C##AINT
    Users:      C##BMR2
C##A       3 C#       X  C##AINT      8    17     17  4Nov95     MANAGEMENT
    Subgroups:  C##AAPPC C##ACONF C##AJRNL C##ARACF C##BRACF C##DELET MVS1
    Subgroups:  SLDMVSS
    Special:    C##AINT  C##BGUS
    Create:     C##AHOU  C##AROB  C##ARO2  C##ASCH  C##ASC3
    Users:      C##AH02  C##ASC2  C##ATST  C##BERT  C##CX01
C##AAPPC   4 C##A          C##A               7      7 14Nov95     APPC DEVELOPME
    Users:      C##ASCH  C##ASC3  C##BCICS C##BGUS  C##CUST
C##ACONF   4 C##A          C##A               4      4 14Nov95
    Users:      C##AHOU  C##AH02  C##BERT  C##BPK2
```

Figure 94. Group profile base segments report with subgroups and connects

For the meaning of the columns see "Group profile tabular display" on page 123.

When **Full detail form** is selected along with the **Show segments** and **All** options, a form-oriented wide print report is generated with results like the report shown in Figure 95 on page 132.

```
RACF groups complex DINO     12Sep2000  16:55 ADMIN    BASE                                                    page    1
All profiles


= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

RACF GROUP                   ADMIN
Group nesting level          3
Superior group               SYSUSER  GRP =QA CNG SCOPE PROFILE
Owner                        SYSUSER                    GRP =QA CNG SCOPE PROFILE
Installation data            GRP =QA CNG SCOPE PROFILE

User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt    RI Name                InstData
-------------------------------------------------------    -- ----                --------
ADM1     USE             READ                            R  USR =QA OW=ADMIN    USR =QA CNG SCOPE PROFILE
ADM2     USE             NONE                            R  USR =QA OW=ADMIN    USR =QA CNG SCOPE PROFILE
FIN1     USE             NONE                            R  USR =QA OW=FINANCE  USR =QA CNG SCOPE PROFILE
FIN2     USE             NONE                            R  USR =QA OW=FINANCE  USR =QA CNG SCOPE PROFILE


Safeguards                           Statistics
----------                           ----------
Terminal use authorization   No      Creation date               16Mar1997
Universal access authority           Universal group             No

= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

RACF GROUP                   AJV
Group nesting level          3
Superior group               SYSAUTH  AUTHORIZATION GROUPS
Owner                        SYSAUTH                    AUTHORIZATION GROUPS
Installation data            JAVA FOR OS390 INSTALL


Safeguards                           Statistics
----------                           ----------
Terminal use authorization   No      Creation date               25Jul1998

= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

Figure 95. Group profile report with full detail, segments, and all options set

RA.D DATASET - Dataset profiles

The Dataset profiles display shows profiles rather than the data sets protected by them. To find about protection for a particular data set, see "RA.3.1 Profiles - Profiles with their data sets" on page 196 and "RA.1 ACCESS - Access Check" on page 184

Simple selection functions

You can use the simple selection panel to add a new profile or segment or to select which profiles to view.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Data set Selection
Command ===> ____________________________________________________   _ start panel

_   Add new DATASET profile or segment

Show dataset profiles that fit all of the following criteria
Dataset profile . . SYS1.**_____________________________________  1 1 EGN mask
Owned by  . . . . . ________     (group or userid, or filter)       2 Exact
High level qual . . ________     (qualifier or filter)              3 Match
Installation data . ____________________ (substring or *)          4 Any match

Additional selection criteria
/  Profile fields     /  Access list      _  Segment presence  _  Absence

Output/run options
_  Show segments      _  All              _  Enable full ACL   _  Specify scope
   Print format       _  Customize title  _  Send as email
   _  Background run  _  Full detail form _  Sort differently  _  Narrow print
   _  Print ACL       _  Resolve to users _  Incl operations   _  Print names
```

Figure 96. Simple dataset profile selection

For information on adding a profile or segment with the **Add new DATASET profile or segment** option, see "Add new DATASET profile or segment" on page 144.

Table 80 describes the available selection criteria.

Table 80. Data set selection criteria field descriptions

Selection criteria field	Description
Dataset profile	If the EGN mask option is selected: an EGN filter to select data set profiles can be used. You can use * in the first qualifier, *SYS*.** to see all z/OS profiles. If **Exact** is selected, you must specify the name of the data set profile in this field.
EGN mask/Exact/Match/ Any match	This field specifies the matching criteria. • **EGN mask** means the query interprets the profile name as an EGN filter (* and % characters are expanded). • **Exact** selects the exact RACF profile. • **Match** treats the profile field as a resource name and selects the profile that best matches the resource name. • **Any match** treats the profile field as a resource name and selects all profiles that match the resource name.
Owned by	Specify an OWNER name as a selection criteria. The owner can be a user or group.
High level qual	The first qualifier of the profile, modified by ICHCNX00 if present.
Installation data	Find occurrence anywhere in the installation data. You cannot use a filter for this field. The search is performed as a *substring scan*.

Table 81 describes the additional selection criteria types that can be specified. Enter / or S in the selection field for the criteria type. After you press enter, the panels to specify the criteria for each selected type are shown in sequence.

Table 81. Types of additional data set selection criteria - field descriptions

Field	Description
Profile fields	If this field is selected, you can specify additional selection criteria based on the contents of profile fields, except fields that relate to connects and segments. The selection panel is shown in "Additional selection - Profile fields" on page 136. If the field is not selected, the **Profile fields** selection criteria are not used but are saved for later use as long as you remain in **RA.D**.
Access list	If this field is selected, you can specify additional selection criteria based on the contents of the access list (ACL). The selection panel is shown in "Additional selection - Access list" on page 138. If the field is not selected, those selection criteria are not used but are saved for later use when you remain in **RA.D**.

Table 81. Types of additional data set selection criteria - field descriptions (continued)

Field	Description
Segment presence	If this field is selected, you can specify additional selection criteria based on the presence of application segments. When you select this option, segment selection and field selection panels open for specifying the criteria. If the output option **Show segments** has also been selected, the Segment presence selection criteria panel only shows the base segment of profiles that have the specific non-base segment. If **Segment presence** field is not selected, the selection criteria are not used but are saved for later use if you remain in **RA.D**.
Segment absence	If this field is selected, absence of a segment can be specified as an additional selection criterion. If the field is not selected, the selection criteria are not used, but are saved for later use if you remain in **RA.D**.

Table 82 describes the options for the report job and data formats. Enter / or S in the entry field to select an option.

Table 82. Data set report format and run options

Option	Description
Show segments	Select this option select the application segments that to be selected or excluded based on segment field values. If the field is not selected, the segment subset is not used but is saved in your ISPF profile for later use. This flag setting is saved in your ISPF profile.
All	Select this option with **Show segments** to show all segments for the selected profiles.
Enable full ACL	Select this option to gather the information necessary to add system-wide operations and default connects to universal groups to the access list. This option implies a full database read. If the **Print format** option is selected, the **Enable full ACL** format option only applies if **Print ACL** has also been selected or implied.
Specify scope	Select this option to limit the results to the scope of a user ID or group.
Print format	Select this option to format the data in print format instead of ISPF display format. This flag setting is saved in your ISPF profile and is shared by all RA options showing it. The options behind and below only apply if this one has been selected. See also “Print format” on page 145.
Customize title	If this field is selected together with **Print format**, you can change the subtitle for the selection. You can also add an extra title that is saved in your ISPF profile, including your company name, department, and phone number for example. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.
Send as email	If this field is selected along with the **Print format** field, then a panel opens for specifying the email address destination for this report. The **Send as email** option only works if the SMTP options have been configured using the SETUP OUTPUT function. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.

Table 82. Data set report format and run options (continued)

Option	Description
Background run	If this field is selected together with **Print format**, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.
Full detail form	If this field is selected together with **Print format**, then at a form-oriented subpage (one per profile) is used to include details. The subpages (profiles) are separated by horizontal dashed lines. The **Full detail form** setting implies the **Print ACL** and **Print names** settings. If the **Full detail form** field is not selected, each segment type is shown in its own tabular report. Sample results are shown in "Print format" on page 145. This flag setting is saved in your ISPF profile. If you have requested segments, they are shown on the same page with the other profile information.
Sort differently	If this field is selected together with **Print format**, then you can change the sort order using this option. This flag setting is saved in your ISPF profile. **Note:** If data is sent to an ISPF display panel, you can change the sort order from the panel by issuing the SORT primary command on the command line.
Narrow print	If this field is selected together with **Print format**, then the page width is limited to 79 characters, independent of the actual print file record length. If the field is not selected, then the page layout you specify must support a width of 132. However, the length can extend beyond that if the print file has a larger record length. This flag setting is saved in your ISPF profile and is shared by all panels that provide this option.

You can specify additional options for formatting and printing ACL data by selecting the options listed in Table 83. The settings for these options are saved in your ISPF profile.

Table 83. Format and print options for ACL data

Option	Description
Print ACL	If this field is selected along with the **Print format** field, then the access list is printed. The exact output format depends on the **Print names** and **Narrow print** settings. You can change the default sort order (by descending access) by selecting the **Sort differently** field. To print the access list in resolved form, use the **Resolve to users** field. If this field is not selected, the ACL information is not included in the results, greatly reducing the number of lines in the report. The **Print ACL** option is automatically implied if the **Full detail form** option is selected. By not printing the access list, the number of output lines can be greatly reduced.

Table 83. Format and print options for ACL data (continued)

Option	Description
Resolve to users	If this field is selected along with the **Print format** and **Print ACL** or **Full detail form**, then the access list is printed resolved to individual user IDs. This format takes into account the way RACF works with user and group permits and connect groups. The access list print can be further extended by selecting the **Incl operations** or **Print names** field.
Incl operations	The access list print includes access through the group-operations attribute if this field is selected along with any of the following fields **Print format** and **Print ACL** or **Full detail form** and **Resolve to users**. Depending on the setting for the **Enable full ACL** option, system-wide operations can also be included.
Print names	If this field is selected along with **Print format** and **Print ACL**, then the access lists are printed with names and installation data added. Only the first part of the installation data is printed, depending on the setting of option **Narrow print**. The **Print names** setting is implied if the **Full detail form** option is selected.

Additional selection - Profile fields

When the **Profile fields** option is selected, another selection criteria panel opens to specify additional selection criteria based on the profile list fields. This panel is shown in Figure 97.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Data set Selection
Command ===> ____________________________________________________________________
like SYS1.**
Specify additional selection criteria:
Profile properties
Creation date . . . __   ___________ (date: yyyy-mm-dd/ddMMMyyyy/TODAY-nnn)
On volume . . . . . ________     (disk/tape volser or filter)
Complex . . . . . ________     (complex name or filter)
Level . . . . . __   __      (installation defined resource level)

Enter "/" to specify inclusion criteria
/  Generic       /  Warning mode    /  Erase on scratch   /  Tape data set
/  Discrete      /  No warning      /  No erase           /  No tape data set

Enter "/" to limit       UACC or ID(*)       Success audit     No failure audit
_  Queued commands       __ _ 1. None        _ 1. Never        _ 1. Read
_  Userdata                   2. Execute        2. >=Read         2. <=Update
_  Universal access           3. Read           3. >=Update       3. <=Control
_  Unconditional ID(*)        4. Update         4. >=Control      4. <=Alter
                              5. Control        5. Alter          5. Ignore
                              6. Alter          6. Ignore
                              7. Ignore UACC
```

Figure 97. Additional data set profile selection - profile fields

In this example, an additional criterion has been added that only profiles with a UACC of READ or higher are to be shown.

The **Enter "/" to specify inclusion criteria** selection group contains option pairs that are selected by default. Based on the default settings, both generic and discrete profiles are to be shown in the report. If the **Enter "/" to limit** option is selected,

only those profiles with the characteristics specified are selected–generic and discrete profiles are not automatically included.

Table 84 describes the profile selection criteria supported for the Data set selection report.

Table 84. RACF Data set selection report - Profile selection criteria

Criteria	Description
Creation date operator	Use the following operators to select data based on the creation date. • < and <= for dates on or before the date specified. • > or >= for later dates. • = for exact dates • ¬= and <> for all but the specified date.
Creation date	The date the profile was defined. The date can be specified in any of the following formats: *ddmmmyyyy*, *01jan1998* for example. *yyyy-mm-dd*, *1998-01-01* for example. *TODAY* TODAY-*xx* where *xx* is a number of days. *DUMPDATE* or DUMPDATE-*xxx* (*DUMPDATE* is the database unload date)
On volume	Discrete profiles with a volume serial.
Complex	In a complex with this name, or a matching complex if a filter is used.
Level operator	Use the operator to determine a level present in the profile. Use < and <= for selection less than or equal to the level, > or >= for high level, = for exact level, ¬= and <> for all but the specified level.
Level	This numeric field indicates the data set level. This level is not set or updated by IBM utilities, but can be used by the installation.
Generic	Show generic profiles
Discrete	Show discrete profiles
Warning mode	Show profiles in warning mode
No warning	Show profiles not in warning mode
Erase on scratch	Show profiles with Erase
No erase	Show profiles without Erase
Tape data set	Show tape data set profiles
No tape data set	Show non-tape data set profiles.
Queued commands	Show only profiles that have one or more commands in the queue.
Userdata	Show only profiles with `userdata.`
Universal access	When this field is selected and Unconditional ID(*) is not, the UACC or ID(*) selection only applies to UACC. When both or neither are selected, the selection applies to UACC and ID(*).
Unconditional ID(*)	When this field is selected and Universal Access is not, the UACC or ID(*) selection only applies to ID(*). When both or neither are selected, the selection applies to UACC and ID(*).

Table 84. RACF Data set selection report - Profile selection criteria (continued)

Criteria	Description
UACC or ID(*)	Show all data set profiles with the specified UACC or an ACL entry with `ID(*)` that has the specified access level matching the operator value specified in the entry field.
Success audit	Show only profiles with this audit setting or higher.
No failure audit	Show only profiles with this audit setting or lower.

Additional selection - Access list

When the **Access list** option is selected, another selection criteria panel opens to specify additional selection criteria based on the access list fields. This panel is shown in Figure 98.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                      zSecure Suite - RACF - Data set Selection
Command ===>
like SYS1.** with UACC or ID(*)>=READ
Specify additional selection criteria:
Find a combination of the following in the access list
# permits . . . . . __   ______              (operator: < <= > >= = <> ¬= )
# conditional permits __   ______            (operator: < <= > >= = <> ¬= )
Id on access list . ________                 (*, group or userid, or filter)
When resource . . . ____________________     (resource name or filter)
Access level  . . . __ _   1. None        When class  . . _  1. PROGRAM
                           2. Execute                       2. CONSOLE
                           3. Read                          3. APPCPORT
                           4. Update                        4. TERMINAL
                           5. Control                       5. JESINPUT
                           6. Alter                         6. SERVAUTH
                           7. Ignore                        7. Present
                                                            8. Ignore

Access list filtering
_   Only show matching ACL entries
```

Figure 98. Additional data set profile selection - access list

Table 85 describes the access list selection criteria supported for the Data set selection report.

Table 85. Data set selection report - Access List selection criteria

Criteria	Description
# permits	Match records based on the number of permits a profile has.
# conditional permits	Match records based on the number of conditional permits.
Id on access list	Match records that have the specified user or group ID value included on the access list. You can use the following filters in the ID specification: `%` for one character, `*` for one or more characters, and `:` for a substring scan. This value is not used for selection based on access that a user has through a group
When resource	You can select all data set profiles that have a conditional access list that includes the specified string in the resource name for the condition. You can use the following filters to specify this value: `%` for one character, `*` for one or more characters, and `:` for a substring scan.

Table 85. Data set selection report - Access List selection criteria (continued)

Criteria	Description
Access level Operator	Use the operator for selection based on the access level present in the ACL. • < and <= for less than or equal to the specified access level. • > or >= for higher access. • = for exact access. • ¬= and <> for all but the specified access level.
Access level	Show all data set profiles with at least one permit with an access level satisfying the Access level Operator.
When class	Show all data set profiles with a conditional access involving the class indicated.
Only show matching ACL entries	Show a subset of the access list, consisting of the access list entries that match all of the criteria selected on this panel.

Dataset profile tabular display

A sample data set profile display is shown in Figure 99.

```
zSecure Admin DATASET overview                          Line 1 of 3
Command ===>                                              Scroll===> CSR
like SYS1.** with UACC or ID(*)>=READ          2 Feb 1999 00:05
   Profile key                                 Type    UACC    Owner    S/F W
__ SYS1.BRODCAST                               GENERIC UPDATE_ SYSPROG_ __R _
__ SYS1.CMDLIB                                 GENERIC READ___ SYSPROG_ U_R _
__ SYS1.LPALIB                                 GENERIC READ___ SYSPROG_ U_R _
```

Figure 99. Dataset profile display

The following fields of interest are shown.

Table 86. DATASET overview panel fields of interest

Field	Description
Profile key	The name of the data set profile. This value is a data set EGN mask.
Type	The profile type, one of GENERIC, VSAM, NONVSAM, MODEL, or TAPE.
UACC	Universal Access Level
Owner	Owning user or group. Together with QUAL, this value determines who can maintain the profile.
S	The lowest access level that results in auditing for successes.
F	The lowest access level that results in auditing for failures.
W	Profile is in Warning mode

You can view additional fields by scrolling to the right.

```
zSecure Admin DATASET overview ---------------------------- Line 1 of 3
Command ===>                                                Scroll===> CSR
like SYS1.** with UACC or ID(*)>=READ          2 Feb 1999 00:05
   Profile key                                 E SgF ID(*)  Complex  Notify
__ SYS1.BRODCAST                               _ ___        DINO     ________
__ SYS1.CMDLIB                                 _ ___        DINO     ________
__ SYS1.LPALIB                                 _ ___        DINO     ________
****************************** BOTTOM OF DATA ********************************
```

Table 87 describes the additional fields.

Table 87. DATASET overview panel - field descriptions

Field	Description
E	Erase-on-scratch flag
SgF	Global, or auditor setting for success and failure auditing.
iD(*)	Shows the access to this profile for `ID *`, which includes all RACF-defined users and groups, except for user IDs with the `RESTRICTED` attribute. This field only shows unconditional access.
Complex	Name for security data base
Notify	User to be notified of violation
Seclabel	Security label
RETPD	Retention period: days protection provided
CreateDat	Definition date
QUAL	Qualifier as modified by naming convention (`ICHCNX00` and `ICHCNV00`). This value together with `OWNER` determines who can maintain the profile.
Lv	The data set level. This level is not set or updated by IBM utilities, but can be used by the installation.
Pri	The relative audit priority for this profile.
InstData	Installation data. To modify this field it is easier to use the MI line command.

Dataset profile detail display

Select any profile on the data set profile table display to see the detail view. You can select entries by putting the cursor on the first character of a row selection field and pressing **Enter**, or by explicitly typing S and pressing **Enter**.

```
zSecure Admin DATASET overview ---------------------------- Line 1 of 43
Command ===>                                                 Scroll===> CSR
like SYS1.** with UACC or ID(*)>=READ          2 Feb 1999 00:05

  Identification                                                    DINO
  Profile name                 SYS1.CMDLIB
  Type                         GENERIC
  Volume serial list
_ Effective first qualifier    SYS1                          MOST SUPERIOR GRO
_ Owner                        SYSPROG_                      SYSTEM PROGRAMMIN
  Installation data            ____________________________________________

  User     Access  ACL id   When               Name                 InstData
_ -group-  ALTER__ SYSPROG_ ________ __________                      SYSTEM PRO
_ -group-  READ___ C##A____ ________ __________                      MANAGEMENT
_ -group-  READ___ SYS1____ ________ __________                      MOST SUPER
_ C##QARUN NONE___ C##QARUN ________ __________ USER RUNT TESTS      ONDER DEZE

  Safeguards                         Other permissions
  Erase on scratch             No_   Allow all accesses    WARNING No_
  Audit access success/failures U R  Universal access authority    READ___
  Global audit success/failures ___  Resource level                _0
  User to notify of violation  ________
  Days protection provided #   _____

  Mandatory Access Control           Statistics
  Security label               ________ Creating user's connect group SYSPROG
  Security level                     Creation date                 28Feb98
  Categories list

  UsrNm   Flg UsrData
_ EXAMPLE  00 USRDATA MAY BE SHOWN HERE
  CKGRACF authority requirement
_ Authority setting DUAL set by C##BGUI at 18 Nov 1997 16:02
  Timed commands waiting for execution
_ Queued command (PR): CMD AT 14Apr2000 PERMIT   'SYS1.CMDLIB' CLASS(DATASET) G
  Commands requiring administrator action
_ Queued command (R): CMD AT 12Oct1999 PERMIT   'SYS1.CMDLIB' CLASS(DATASET) GE
  Inactive commands
_ Queued command (E): CMD AT 01Jan1999 FOR 2 PERMIT   'SYS1.CMDLIB' CLASS(DATAS
  Commands that have been executed
_ Queued command (X): CMD AT 01Jan1999 FOR 500 PERMIT   'SYS1.CMDLIB' CLASS(DAT
****************************** BOTTOM OF DATA ******************************
```

Figure 100. DATASET profile detail display

The fields described in Table 88 might be shown depending on the SETUP options and data availability.

Identification section

Table 88. Dataset Profile Detail panel - Identification section panel

Field	Description
Identification	To the far right, the complex name is shown.
Type	The profile type, one of GENERIC, VSAM, NONVSAM, MODEL, or TAPE.
Profile name	The key of the DATASET profile.
Volume serial list	Data set volume serials for discrete profiles.
Effective first qualifier	The first qualifier (user or group), as modified by the installation naming convention exit and table (ICHCNX00 and ICHNCV00), followed by the user name and the user or group installation data.
Owner	The owning user or group, followed by the user name and the user or group installation data.

Table 88. Dataset Profile Detail panel - Identification section panel (continued)

Field	Description
Installation data	Installation data field of the profile. If the installation data is too wide for the display, you can view and edit it more easily using the **MI** line command on the tabular display.

Access list fields. Table 89 describes these fields.

Table 89. Dataset Profile Detail panel - Access list fields

Field	Descriptions
User	User ID authorized through access list.
Access	Access level.
ACL id	ID on access list.
When	Conditional access applies (class / resource).
Name	Name of the user, if applicable.
InstData	Installation data of the user or group

The ACL data can be shown in several different formats. For example, the groups can be expanded to show the user IDs, duplicate references can be resolved, and operations access can also be shown. See "Access list display modes - reference material" on page 30 and "Managing the Access List display panel" on page 81 for information on these formats.

Safeguards fields. Table 90 describes these fields.

Table 90. DATASET Profile detail display - Safeguards fields

Field	Description
Erase on scratch	This flag shows whether data security erasure has been requested at the profile-level. Even for 'Yes', the option is only honored if SETROPTS ERASE has also been set.
Audit access success/failures	Two one-letter abbreviations for the access level that is to be audited for successes and failures (violations), respectively. This setting can be changed by the profile owner.
Global audit success/failures	Two one-letter abbreviations for the access level that is to be audited for successes and failures (violations), respectively. Only the auditor can change this setting.
User to notify of violation	Userid that has to receive a message when a violation occurs.
Days protection provided #	The RETPD of tape data sets, checked if the TAPEVOL class is active.

Other permissions fields. Table 91 describes these fields.

Table 91. DATASET Profile detail display - Other permissions fields

Allow all accesses WARNING	The value *Yes* indicates that warning mode is active. This mode implies that all accesses are permitted, but a warning message is indicated if the access normally results in a violation.

Table 91. DATASET Profile detail display - Other permissions fields (continued)

Universal access authority	The profile access level (UACC) that applies to all users, even users not defined in RACF. This access does not apply to users with the `RESTRICT` attribute.
Resource level	The data set level. This level is not set or updated by IBM utilities, but can be used by the installation.

Mandatory Access Control fields. Table 92 describes these fields.

Table 92. DATASET Profile detail display - Mandatory Access Control fields

Security label	Contains the resource security label used in Mandatory Access Control decisions (B1 security).
Security level	Contains the resource security level, which is the minimum level the user requires for reading the data set.
Categories list	Lists all security categories that the user requires for reading the data set.

Statistics fields. Table 93 describes these fields.

Table 93. DATASET Profile detail display - Statistics fields

Field	Description
Creating user's connect group	The then-current connect group of the user who created the data set profile.
Creation date	The date that the profile was created.

Additional, optional properties. Table 94 describes these fields.

Table 94. DATASET Profile detail display - Additional, optional property fields

Field	Description
Audit concern	A concatenation of audit concerns for the profile.
UsrNm	The names of the `userdata` fields, excluding those fields used by `CKGRACF`.
Flg	Flag associated with the `userdata` field
UserData	Contents of the `userdata` field
CKGRACF authority requirement	The authority required to change this DATASET profile by `CKGRACF` (SINGLE, DOUBLE or TRIPLE). That is, the number of administrators who must sanction a command.
Timed commands waiting for execution	Timed commands that have been approved and are now waiting for their execution date (*P*). Commands that have an end date scheduled, remain in this queue until their reversal date (*PR*).
Commands requiring administrator action	The commands that have not been fully authorized yet as per the value specified in **CKGRACF authority requirement** or per the system-wide default access level.
Inactive commands	Requested commands that were not fully authorized and then expired, were withdrawn, or were denied. These inactive commands are included in the audit trail with other commands that were not run.
Commands that have been executed	Commands that were fully authorized and run. These commands are included in the audit trail.

For an explanation of the CKGRACF data, see “RA.2 QUEUED - Queued commands” on page 185 and .

Line commands on a DATASET profile display

When you use the **/** line command to ask which line commands are permitted, the following table opens.

Table 95. Line commands on a DATASET profile display

Command	Meaning	Explanation
AC	Access Check for one user ID or group.	“RA.1 ACCESS - Access Check” on page 184
C	Copy data set profile.	“C - Copy” on page 55
D **DD**	Delete data set profile, or delete a non-base segment.	“D - Delete” on page 58
E	Display event logging.	“E - Event” on page 59
L	RACF `listdsd` command.	The results of the `listdsd` command are presented in a browse panel.
LD	RACF `listdsd DSNS` command.	Operates like the **L** command but also requests display of the data sets covered.
LR	List data sets covered by profile	“LR - List data sets covered via Report” on page 60
MI	Manage `instdata`.	“MI - Manage information” on page 61
MR	Manage `CKGRACF` authority requirements	“MR - CKGRACF mulitple authority requirement” on page 63
MU	Manage installation-defined USERDATA	“RA.3.9 USERDATA - User data management” on page 219
PE	Add or delete permit	“PE - Add or delete permit” on page 69
R **RR**	Recreate data set profile	“R - Recreate a profile” on page 70
S	Show additional information (same as just putting the cursor at the selection field)	“S - Select” on page 72
SE	Show application segments	“SE - Show application segments” on page 72 and “Application segments” on page 145.
X **XX**	Exclude a profile from `FORALL` processing.	“X - Exclude profile line command” on page 74
Z **ZZ**	Select profile for `FORALL` processing.	“Z - Select a profile” on page 74
34	Data Set List Utility	“34 - Data set list utility” on page 74

Add new DATASET profile or segment

You can add a new data set profile or empty segment to the current system with the **Add new DATASET profile or segment** option on the RACF Data set Selection panel (Figure 96 on page 132).

You can also add a new profile by copying an existing one. For details, see “C - Copy” on page 55. If you want to add a dataset profile or segment on another system, you must use a batch job.

Use the following procedure to add a new dataset profile or segment from the RACF Dataset Selection panel.

1. On the RACF Group Selection panel (Figure 86 on page 118), type a / or *S* in the **Add new DATASET profile or segment** field.
2. Press **Enter** to open the Data set Add panel.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Data set Add
 Command ===> ____________________________________________

 Dataset profile . . ____________________________________

 Owned by  . . . . . _______ (may also be set in the follow on update dialog)
 /   Define new DATASET profile

 _   Add DFP segment
 _   Add TME segment
```

Figure 101. Add DATASET profile panel

3. On the Add panel, you can add a new data set profile, add a segment to an existing data set profile, or add a combination of a data set and segment. For information on performing these tasks, see the ISPF panel help.
4. After specifying the field information, press **Enter** to the immediately add the data set or segment on the system where you are logged on.

   The RACF command response is only shown if there is a nonzero return code.

Notes:

1. When the Add panel displays, the default owner is provided to support users that do most of their additions in the same group. This value is stored in your ISPF profile based on previous add data set operations.
2. After the addition operation has successfully completed, a panel opens with the new profile or segments shown with modifiable fields for further customization. The format of this panel is the same as the detail display panel described in “Dataset profile detail display” on page 140.

Application segments

When the **Show segments** option has been selected, or the SE action command is used, application segments are shown.

The DATASET DFP segment shows the field **Resowner**, which is the resource owner (a user or group).

The DATASET TME segment detail display shows the Tivoli Management Environment role access specifications. The segment display shows the number of specifications and the first specification.

Print format

After you select the **Print format** option, a number of additional options are available for selection. The print data can be formatted in either tabular or form-oriented by selecting the **Full detail form** option. The tabular form sacrifices some detail in favor of a readable printout. The print format can either use a print

file width of at least 132 characters, or it can be limited to 79 columns through the **Narrow print** option. The prints can be sorted in another way than by profile name through the **Sort differently** option.

If **Sort differently** is selected, a sort order panel is displayed for each segment type to be shown. Figure 102 shows the sort order panel for the base segment.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Data set Sort Order
Command ===> ____________________________________________________________________
like SYS1.** with UACC or ID(*)>=READ
Specify up to 3 fields to act as
alternate base segment sort order
Select with 1 or / and optionally 2, 3
_ Profile name (default)
_ Qualifier (naming conventions)
_ Profile type
_ Installation data
_ Owner
_ Notify
_ Creation date (descending)
1 Universal access (descending)
_ Warning mode
_ Erase-on-scratch
_ Retention period (descending)
_ Level (descending)
_ By audit priority (descending)
```

Figure 102. Data set sort order panel

In the sort order panels, one can specify up to three sort keys by entering 1, 2, or 3 in front of the sort criteria. If you want to sort on just one column, it is also possible to use a / instead of 1.

Figure 103 shows an example of wide tabular print output of dataset profile base segments, sorted by descending universal access:

```
zSecure Admin DATASET Overview - complex DINO   14Sep2000  15:59                                                    page    1
like SYS1.** with UACC or ID(*)>=READ, sorted by uacc

Profile key                              TWE UACC    Owner    QUAL     S/F RETPD Created Notify  Lv InstData
SYS1.BRODCAST                            G   UPDATE  SYSPROG  SYS1       R        7Nov95
SYS1.CMDLIB                              G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LOCAL.LINKLIB                       G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LOCAL.VTAMLIB                       G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LPALIB                              G   READ    SYSPROG  SYS1     U R        7Nov95
```

Figure 103. DATASET Overview Report panel

```
zSecure Admin DATASET Overview - complex DINO   14Sep2000  15:59                                                    page    1
like SYS1.** with UACC or ID(*)>=READ, sorted by uacc

Profile key                              TWE UACC    Owner    QUAL     S/F RETPD Created Notify  Lv Pri InstData
SYS1.BRODCAST                            G   UPDATE  SYSPROG  SYS1       R        7Nov95             10
     Concern:  Verify why UACC>=UPDATE
SYS1.CMDLIB                              G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LOCAL.LINKLIB                       G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LOCAL.VTAMLIB                       G   READ    SYSPROG  SYS1     U R       28Feb98
SYS1.LPALIB                              G   READ    SYSPROG  SYS1     U R        7Nov95
```

The TWE columns indicate `Type`, `Warning`, and `Erase` status, respectively. For the meaning of the other columns see "Dataset profile tabular display" on page 139.

When *Narrow print* is checked, the output is almost the same, except that installation data (if any) is on a separate line. This changes if *Print ACL* is also selected, the output is shown with each access level on a separate line:

```
RACF DATASET profiles  - complex DINO     14Sep2000  16:02           page    1
like SYS1.** with UACC or ID(*)>=READ, sorted by uacc

Profile key                    TWE UACC    Owner    S/F RETPD Created Notify Pri
SYS1.BRODCAST                  G   UPDATE  SYSPROG    R        7Nov95         10
     Concern:  Verify why UACC>=UPDATE
     Alter:    SYSPROG
SYS1.CMDLIB                    G   READ    SYSPROG  U R       28Feb98
     Alter:    SYSPROG
     Read:     C##A SYS1
     None:     C##QARUN
SYS1.LOCAL.LINKLIB             G   READ    SYSPROG  U R       28Feb98
     Alter:    SYSPROG SYS1
     Read:     C##A
     None:     C##QARUN
SYS1.LOCAL.VTAMLIB             G   READ    SYSPROG  U R       28Feb98
     Alter:    SYSPROG SYS1
     Read:     C##A
     None:     C##QARUN
SYS1.LPALIB                    G   READ    SYSPROG  U R        7Nov95
     Alter:    SYSPROG
```

When **Full detail form** is also selected, the profile forms are separated by dashed lines. When **Resolve to users** has been selected, the access list is resolved to user IDs (matrix).

```
SYS1                           DINO     14Sep2000  16:42 BASE          page    1
key SYS1.ACDS


= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

DATASET profile name          SYS1.ACDS
Type                          GENERIC
Effective first qualifier     SYS1                          MOST SUPERIOR GROUP
Owner                         SYSPROG                       SYSTEM PROGRAMMING

User     Access  ACL id   When               Name                 InstData
------------------------------              ----                 --------
C##BMR1  ALTER   SYSPROG                     MIKE REED           INSTDATA
C##BPK1  ALTER   SYSPROG                     PETE KENDALL
C##BPK2  ALTER   SYSPROG                     PETE KENDALL
DEPT     ALTER   SYS1                        USR =QA OW=SYS1      USR =QA CNG
DEPT1    ALTER   SYS1                        USR =QA OW=DEPT      USR =QA CNG
DEPT2    ALTER   SYS1                        USR =QA OW=DEPT      USR =QA CNG
DFHSM    ALTER   SYS1
DFRMM    ALTER   SYS1                        DFRMM STARTED TASK U
IBMUSER  ALTER   SYS1                        IBM DEFAULT USER
OSA      ALTER   SYS1                        OSA STARTED TASK USR
STRTASK  ALTER   SYS1                        DIV STARTED TASK USR
SYSPSTC  ALTER   SYSPROG                     STC USER SYSPROG
- any -  READ    *
C##QARUN NONE    C##QARUN                    USER RUNS TESTS      U

Safeguards                            Other permissions
----------                            -----------------
Erase on scratch              No      Allow all accesses    WARNING No
User to notify of violation           Universal access authority    NONE
Audit success access level    UPDATE  Resource level                0
Audit failures access level   READ

Mandatory Access Control              Statistics
------------------------              ----------
Security label                ........ Creating user's connect group SYSPROG
Security level                         Creation date                11Nov1998
Categories list
```

RA.R RESOURCE - General Resource profiles

The General Resource profiles panel provides access to simple profile selection functions. Use these functions to add a new profile or segment or select from profiles in a class like `FACILITY` or `GCICSTRN`.

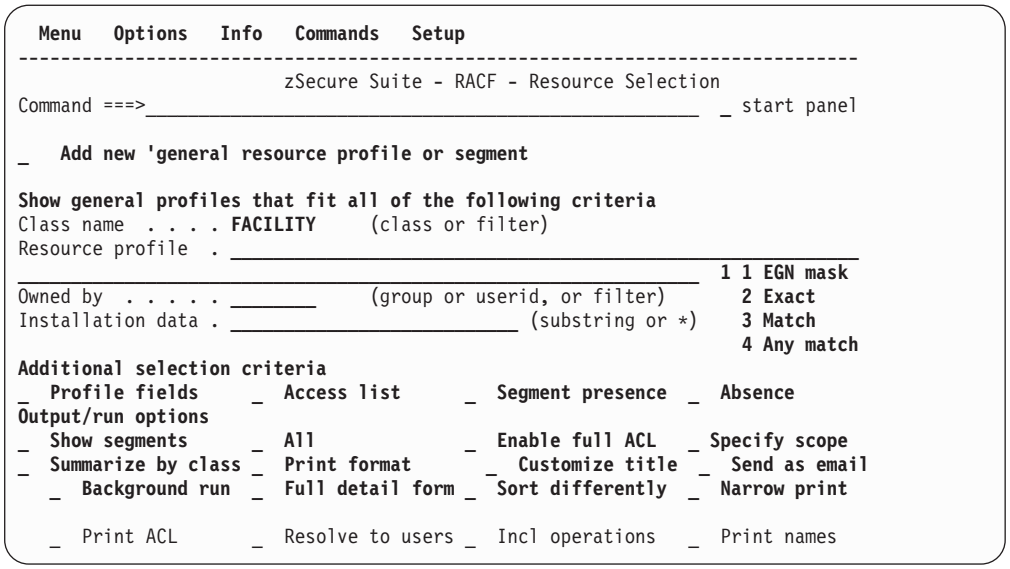


Figure 104. Simple resource profile selection

Table 96 describes the selection criteria on the RACF resource selection report panel.

Table 96. Resource selection - selection criteria

Class name	Limit the display of profiles to a CLASS defined in the CDT. For example, use JES* to show JESJOBS and JESSPOOL. If left blank, all resource classes are eligible.
Resource profile	If the EGN mask option is selected: an EGN filter to select resource set profiles can be used. If Exact is selected, the name of the resource profile must be specified.
EGN mask /Exact/Match /Any match	If the EGN mask is selected, the query interprets the profile name as an EGN filter (*- and %-characters are expanded). Exact selects the exact RACF profile. Match treats the profile field as a resource name and selects the best profile that could match the resource name. Any match treats the profile field as a resource name and selects all profiles that could match the resource name.
Owned by	Indicates the specified owner. The owner can be a user or group. You can use a filter specification in this field.
Installation data	Find occurrence anywhere in the installation data. A filter is not permitted. When this action runs, it performs a *substring scan*.

Additional selection criteria can be requested by entering / or *S* in the entry field for the following options.

Profile fields	For more selection criteria (except referring to connects and segments), use this checkbox. The selection panel is shown in "Additional selection - Profile fields" on page 156. If the field is not selected, the **Profile fields** selection criteria are not used but are saved for later use as long as you remain in **RA.R**.
Access list	For selection based on the contents of the access list (ACL). The selection panel is shown in "Additional selection - Access list" on page 158. If the field is not selected, those selection criteria are not used, but are saved for later use as long as you remain in **RA.R**.

Segment presence	If this field is selected, criteria can be specified for the presence of application segments. A segment selection panel and a segment field selection panel are shown. Only segments that contain data that is shown by the product are available. For example, the SSIGNON segment contains only the SSKEY field which is not shown because it is considered sensitive and is not supported for selection. unless the output option **Show segments** has also been selected, selecting the **Segment presence** option results in showing only the base segment of profiles that have the specific non-base segment.If the field is not selected, the selection criteria are not used but are saved for later use as long as you remain in **RA.R**.
Segment absence	If this field is selected, absence of a segment can be specified as an additional selection criterion. If the field is not selected, the selection criteria are not used but are saved for later use as long as you remain in **RA.R**.

Table 97 lists the output and run options you can specify.

Table 97. Resource selection - output and run options

Show segments	Show a selectable set of application segments for specifying select and exclude criteria based on segment field values. If this option is not selected, the segment subset is not used but is saved in your ISPF profile for later use. This flag setting is saved in your ISPF profile.
All	This option can be used with **Show segments** to show all segments for the selected profiles.
Enable full ACL	This checkbox can be used to gather the information necessary for adding system-wide operations and default connects to universal groups to the access list. It implies a full database read. If **Print format** is selected, it is only effective if **Print ACL** has also been selected or implied.
Specify scope	If this field is selected (with a /), you can limit the output to the scope of a userid or group.
Summarize by class	If this field is selected, the resource profiles are grouped by resource class. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.
Print format	If this field is selected, output is in print format instead of ISPF display format. This flag setting is saved in your ISPF profile and is shared by all RA options showing it. The other print-related options are only available for selection if the **Print format** option is selected. See also “Print format” on page 170.
Customize title	If this field is selected together with **Print format**, you can change the subtitle for the selection as well as add an extra title that is saved in your ISPF profile, including your company name, department, and phone number for example. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.
Send as email	If this option is selected along the **Print format** option, then a panel opens for specifying the email address destination for this report. The **Send as email** option only works if the SMTP options have been configured using the SETUP OUTPUT function. This flag setting is saved in your ISPF profile and is shared between all RA options showing it.

Table 97. Resource selection - output and run options (continued)

Background run	If this field is selected together with **Print format**, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared by all `RA` options showing it.
Full detail form	If this field is selected together with **Print format**, forms (one subpage per group, separated by dashed lines) are used to include details. This selection implies selections for the **Print connects**, **Print names**, and **Print subgroups** options. This flag setting is saved in your ISPF profile. If you have requested segments, they are shown on the same page with the other group information. If the **Full detail form** field is not selected, each segment type is shown in its own tabular report. Sample output is shown in "Print format" on page 129.
Sort differently	If this field is selected together with **Print format**, then an alternate sort order can be selected. If you want to change the sort order in an ISPF display panel (**Print format** not selected), you can use the `SORT` primary command in the actual display. This flag setting is saved in your ISPF profile.
Narrow print	If this field is selected together with **Print format**, then the width of the page is limited to 79 characters, independent of the actual print file record length. If the field is not selected, then the page layout you specify must support a width of 132. However, the length can extend beyond that if the print file has a larger record length. This flag setting is saved in your ISPF profile and is shared by all panels showing this option.
Print ACL	If this option is selected along with the **Print format** option, then the Connects are printed. The exact output format depends on the **Print names** and **Narrow print** settings. The default sort order (by descending access) can be changed by selecting the **Sort differently** option. To print the access list in resolved form, use the **Resolve to users** option. This option is implied by **Full detail form**. By not printing the access list, the number of output lines can be greatly reduced. This flag setting is saved in your ISPF profile.
Resolve to users	If this option is selected along with the **Print format** and **Print ACL** or **Full detail form**, then the access list is printed resolved to individual user IDs, taking into account the way RACF works with user and group permits and connect groups. The access list information can be further extended by using the **Incl operations** and **Print names** options. This flag setting is saved in your ISPF profile.
Incl operations	If this field is selected along with **Print format** and **Print ACL** or **Full detail form** and **Resolve to users**, then the printed access list data includes access through the group-operations attribute. When `Enable full ACL` is selected, system-wide operations are also included. This flag setting is saved in your ISPF profile.
Print names	If this field is selected along with **Print format** and **Print ACL**, then the access lists are printed with names and installation data added. Only the first part of the installation data is printed, depending on the setting of option **Narrow print**. If **Narrow print** is selected, the revoke and resume dates for the Connect are not visible. This flag is implied by **Full detail form**. This flag setting is saved in your ISPF profile.

For more information about general resource reports, see the following topics:

- "Resource profile tabular display" on page 151

Resource profile tabular display

In the selection panel above, all profiles in the class FACILITY are being requested. This results in the following overview:

```
zSecure Admin General resource overview ------------------ Line 7 of 290
Command ===> _____________________________________________ Scroll===> CSR
Class FACILITY                                  2 Feb 1999 00:05
   Class    Profile key                              T UACC    Owner    S/F W
__ FACILITY $CNG.CMD.ACCESS.ALL                       NONE___ SYSAUTH_ __R _
__ FACILITY $CNG.CMD.AUTHORITY                        NONE___ SYSAUTH_ __R _
__ FACILITY $CNG.CMD.AUTHORITY.C##QA002               NONE___ SYSAUTH_ __R _
__ FACILITY $CNG.CMD.AUTHORITY.*                    G NONE___ SYSAUTH_ __R _
__ FACILITY $CNG.CMD.CMD.ASK.*                      G UPDATE_ SYSAUTH  R_R _
s_ FACILITY $CNG.CMD.CMD.EX.ALTUSER                   UPDATE_ SYSAUTH  R_R _
__ FACILITY $CNG.CMD.CMD.EX.*                       G UPDATE_ SYSAUTH  R_R _
__ FACILITY $CNG.CMD.CMD.REQ.CONNECT                  NONE___ SYSAUTH  R_R _
```

By scrolling to the right, additional fields can be displayed. The following fields of interest are shown:

Class	The profile class
Profile key	The profile name
T	The profile type: a *G* for a generic profile and blank otherwise.
UACC	The universal access level for the profile.
Owner	Owner
S	Audit success level
F	Audit failure level
W	Profile is in Warning mode
SgF	Global, or auditor setting for success and failure auditing.
ID(*)	This field shows the access to this profile for ID *. This access level applies to all RACF-defined users and groups, except for user IDs with the RESTRICTED attribute. This field only shows unconditional access.
Complex	Name for security data base
Notify	User to be notified of violation
Seclabel	Security label
CreateDat	Definition date
ApplData	Application data. The data listed depends on the profile class.
Lv	The resource level. This level is not set or updated by IBM utilities, but can be used by the installation.
Pri	The relative audit priority for this profile.
InstData	Installation data

Resource profile detail display

Select any profile on the resource profile table display to see the detail view. Selection can be done by putting the cursor on the first character of row selection field and pressing **Enter**, or by explicitly typing S there and pressing **Enter**.

A detail display is shown in Figure 105.

```
zSecure Admin General resource overview ------------------- Line 1 of 46
Command ===>                                                 Scroll===> CSR
Class FACILITY                                2 Feb 1999 00:05


  Identification                                                    DINO
  Class                          FACILITY
  Profile name                   $CNG.CMD.CMD.EX.ALTUSER
  Type
  Volume serial list
_ Owner                          SYSAUTH_                      AUTHORIZATION GRO
  Installation data              ________________________________________________
  Application data               ________________________________________________

  User     Access  ACL id   When                Name                 InstData
_ -group-  ALTER__ SYSPROG_ ________ __________                       SYSTEM PRO
_ C##QA001 CONTROL C##QA001 ________ __________ QA SUBJECT 001
_ -group-  UPDATE_ C##ARACF ________ __________                       DIRECT LIV
_ -group-  UPDATE_ C##QA___ ________ __________                       Q.A. TESTS

  Safeguards                              Other permissions
  User to notify of violation    ________ Allow all accesses    WARNING No_
  Audit access success/failures R R       Universal access authority    NONE___
  Global audit success/failures ___       Resource level                _0

  Mandatory Access Control                Statistics
  Security label                 ________ Creation date                 12Mar97
  Security level
  Categories list

  UsrNm   Flg UsrData
_ EXAMPLE  00 USRDATA MAY BE SHOWN HERE AS WELL
  CKGRACF authority requirement
_ Authority setting DUAL set by C##BGUI at 18 Nov 1997 16:03
  Timed commands waiting for execution
_ Queued command (PR): CMD AT 15Apr2000 PERMIT   '$CNG.CMD.CMD.EX.ALTUSER' CLAS
  Commands requiring administrator action
_ Queued command (R): CMD AT 19Oct1999 PERMIT   '$CNG.CMD.CMD.EX.ALTUSER' CLASS
  Inactive commands
_ Queued command (E): CMD AT 03Jan1999 FOR 8 PERMIT   '$CNG.CMD.CMD.EX.ALTUSER'
  Commands that have been executed
_ Queued command (X): CMD AT 02Jan1999 FOR 499 PERMIT   '$CNG.CMD.CMD.EX.ALTUSE
  Other CKGRACF data
_ Internal authority setting DUAL set by C##QARUN at  1 Dec 1998 08:24
****************************** BOTTOM OF DATA ********************************
```

Figure 105. Resource profile detail display

The following fields of interest can be shown (depending on SETUP options, and data availability).

Identification section

Identification	To the far right, the complex name is shown.
Class	The profile class

Type	The profile type, one of GENERIC, VSAM, NONVSAM, MODEL, or TAPE. If this field is left blank, it indicates a DISCRETE profile.
Profile name	The key of the general resource profile. Long names are wrapped.
Volume serial list	Volume serials for discrete `TAPEVOL` profiles
Owner	The owning user or group, followed by the user name and the user or group installation data.
Installation data	Installation data field of the profile. If you need to edit wide data, it is easier to use the MI line command on the tabular display.
Application data	Application data. The meaning of this field depends on the class. If you need to edit wide data, it is easier to use the MI line command on the tabular display.

Access list section

User	Userid authorized through access list
Access	Access level
ACL id	Id on access list
When	Conditional access applies (class and resource name)
Name	Name of the user (if applicable)
InstData	Installation data of the user or group

Members section

The Members section lists the members of the resource profile. It is only shown if applicable.

Safeguards section

User to notify of violation	Userid that has to receive a message when a violation occurs.
Audit access success/failures	Two one-letter abbreviations for the access level that is to be audited for successes and failures (violations), respectively. This setting can be changed by the profile owner.
Global audit success/failures	Two one-letter abbreviations for the access level that is to be audited for successes and failures (violations), respectively. This is the setting that only an auditor can change.

Other permissions section

Allow all accesses WARNING	Shows *Yes* for warning mode. This implies all accesses are permitted but with warning messages where normally a violation would have occurred.
Universal access authority	The profile access level (UACC) that applies to all users, even those not defined in RACF. This access does not apply to users with the `RESTRICT` attribute.
Resource level	The resource level is not set or updated by IBM utilities, but can be used by the installation.

Mandatory Access Control section

Security label	This contains the resource security label used in Mandatory Access Control decisions (B1 security).
Security level	This contains the resource security level, which is the minimum access level the user must have to access the resource.
Categories list	This lists all security categories the user must have to access the resource.

Statistics section

Creation date	This is the date that the profile was created.

Additional, optional properties

Audit concern	A concatenation of audit concerns for the profile.
UsrNm	The names of the `userdata` fields, excluding those fields used by `CKGRACF`.
Flg	Flag associated with the `userdata` field.
UsrData	Contents of the `userdata` field.
CKGRACF authority requirement	The authority required to change this profile by `CKGRACF` (SINGLE, DOUBLE or TRIPLE). This authority level represents the number of administrators who must approve a command before it can be run.
Timed commands waiting for execution	Timed commands that have been approved and are now waiting for their execution date (*P*). Commands that have scheduled end date remain in this queue until their reversal date (*PR*).
Commands requiring administrator action	The commands that have not been fully authorized yet as per the **CKGRACF authority requirement authority** or per the system-wide default value.
Inactive commands	Requested commands that were not fully authorized and then expired, were withdrawn, or were denied. Inactive commands are included in the audit trail with other commands that were not run.
Commands that have been executed	Commands that were fully authorized and run. These commands are included in the audit trail.
Other CKGRACF data	The `userdata` fields used by `CKGRACF` for other purposes. An internal authority requirement can be shown here, typically for `CKGRACF` profiles. This is the authority setting associated with a `CKGRACF` command for which this profile determines the protection. It is not associated with the `CKGRACF` authority setting of this profile itself.

For an explanation of the `CKGRACF` data refer to "RA.2 QUEUED - Queued commands" on page 185 and "MR - CKGRACF mulitple authority requirement" on page 63.

The ACL can be shown in several different formats. For example, the ACL format shown is SORT– the groups can be expanded to the user IDs contained therein, duplicate references can be resolved, and operations access can also be shown. Refer to "Access list display modes - reference material" on page 30 and "Managing the Access List display panel" on page 81 for further explanation.

General Resource Class Overview

The query shown in "Resource profile detail display" on page 152 specifically selected the FACILITY class. If you do not select a specific class the profile overview is preceded by a class overview.

```
zSecure Admin General resource overview ------------------- Line 1 of 53
Command ===>                                                 Scroll===> CSR
All profiles                                        2 Sep 1999 14:49
   Class    Profiles  Generic Discrete Max Len Total Len Max UAC
__ ACCTNUM         3        1        2     175       467 NONE
__ AIMS            2        0        2     133       265 NONE
__ APPCLU         24        1       23     172      3056 NONE
__ APPCPORT       12        0       12     132      1556 NONE
__ APPCSERV        2        1        1     137       270 NONE
__ APPCTP          2        1        1     246       383 READ
__ APPL           18        0       18     198      2490 NONE
__ CCICSCMD        2        0        2     117       228 NONE
__ CONSOLE         4        1        3     180       544 READ
__ CSFKEYS         1        1        0     122       122 NONE
__ CSFSERV         1        1        0     122       122 NONE
__ DASDVOL         3        1        2     135       395 NONE
__ DCEUUIDS        1        0        1     165       165 NONE
__ DIGTCERT       24        0       24     257      5078 TRUST
__ DIGTCRIT        2        0        2     119       238 NONE
__ DIGTNMAP        4        0        4     269       850 NONE
__ DLFCLASS        4        2        2     158       539 NONE
__ DSNR            1        0        1     131       131 NONE
__ FACILITY      385      136      249     670     69663 UPDATE
__ FIELD          89       15       74     194     11431 NONE
__ GCICSTRN        3        0        3     164       470 READ
__ GLOBAL          3        0        3     203       486 NONE
__ GSDSF           1        0        1     182       182 NONE
__ IBMOPC          2        1        1     274       510 NONE
__ JESINPUT        2        0        2     117       221 READ
__ JESJOBS         1        1        0      98        98 READ
__ JESSPOOL       41       41        0     213      7048 READ
__ NETCMDS         2        1        1     630       752 NONE
__ NETSPAN         1        1        0     122       122 NONE
__ NODES          12       11        1     180      1729 CONTROL
__ OPERCMDS       39       29       10     271      7913 READ
__ PERFGRP         1        1        0      98        98 READ
__ PROGRAM        45        0       45    2270     18480 READ
__ PTKTDATA       13        1       12     143      1684 NONE
__ RACFVARS        8        0        8     301      1611 READ
__ ROLE            8        0        8     343      1322 NONE
__ RRSFDATA        9        4        5     267      1488 READ
__ SDSF           33       18       15     216      4839 UPDATE
__ SECDATA         2        0        2    1039      1194 NONE
__ SECLABEL        6        0        6     142       683 NONE
__ STARTED       134      133        1     159     15825 NONE
__ SURROGAT       44        5       39     268      7308 NONE
__ SYSMVIEW        4        1        3     184       676 NONE
__ TAPEVOL        20       14        6     534      4372 READ
__ TERMINAL        4        1        3     147       486 NONE
__ TSOAUTH         7        0        7     207      1085 READ
__ TSOPROC        20        3       17     295      4463 READ
__ UNIXMAP        94        0       94     258     11846 NONE
__ VMCMD           1        0        1     137       137 NONE
__ VMMDISK         5        4        1     118       552 NONE
__ VMPOSIX        12        1       11     181      2038 NONE
__ VTAMAPPL       11        0       11     105      1155 NONE
__ WRITER          1        1        0     142       142 READ
******************************* BOTTOM OF DATA ********************************
```

In this overview, the PROGRAM class has 45 discrete profiles. The SDSF class has 33 profiles, of which 18 are generic and 15 are discrete. The biggest general resource profile is in the PROGRAM class (2270 bytes), and the general resource class that uses the most space is FACILITY. The user, group, and data set profiles

are not listed in this overview. You can view the profiles by selecting any class in the overview. This selection opens the panel listing the profiles in the specified class.

Additional selection - Profile fields

If the *Profile fields* field is selected in the additional selection section, the panel shown in Figure 106 is displayed.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Selection
Command ===> ____________________________________________________________
Class %CIC*
Specify additional selection criteria:Profile properties
Creation date . . . __   ___________ (date: yyyy-mm-dd/ddMMMyyyy/TODAY-nnn)
Complex . . . . . ________     (complex name or filter)
Search words or phrases, separated by commas, use ' 'c to preserve case:
Profile . . . . . ____________________________________________________________
Memberlist  . . . . CEDA_____________________________________________________
Level . . . . . __   __      (installation defined resource level)

Enter "/" to include  Enter "/" to limit  UACC or ID(*)       Show merged
/  Generic            _  Queued cmds      __ _ 1. None        memberlist
/  Discrete           _  Userdata             2. Execute     _  1. No
/  Warning mode       _  Universal access     3. Read           2. Yes
/  No warning         _  Uncond. ID(*)        4. Update         3. Duplicates
                                              5. Control
                                              6. Alter
                                              7. Ignore UACC
```

Figure 106. Advanced resource profile selection

In the example shown, we are looking for profiles in any CICS class that contain the substring *CEDA* in their member lists.

Table 98 describes the advanced selection criteria available for the RACF resource report.

Table 98. RACF resource selection - Advanced selection criteria

Criteria	Description
Creation date operator	Use the operator to determine the date for operator selection. Use < and <= for selection prior to or on the date specified, > or >= for later dates, = for exact dates, ^= and <> for all but the specified date.
Creation date	The date the profile was defined. The date can be specified in any of the following formats: • `ddmmmyyyy`, `01jan1998` for example. • `yyyy-mm-dd` , 1998-01-01 for example. • `TODAY` • `TODAY-xx` where *xx* is a number of days • `DUMPDATE` where *dumpdate* is the database unload date. • `DUMPDATE-xxx`
Complex	In a complex with this name, or a matching complex if a filter is used.
Profile	Text strings that can appear anywhere in the profile, `CEMT,DCMT` for example.
Memberlist	Text strings that can appear in the member list only, `CEMT,DCMT` for example.

Table 98. RACF resource selection - Advanced selection criteria (continued)

Criteria	Description
Level operator	Use the operator to determine a level present in the profile. Use < and <= for selection less than or equal to the level, > or >= for high level, = for exact level, ¬= and <> for all but the specified level.
Level	This numerical field indicates the resource level. This level is not set or updated by IBM utilities, but can be used by the installation.
Generic	Show generic profiles
Discrete	Show discrete profiles
Warning mode	Show profiles in warning mode
No warning	Show profiles not in warning mode
Queued cmds	Show only profiles that have one or more queued commands.
Userdata	Show only profiles with `userdata`
Universal access	When this field is selected and *`Uncond. ID(*)`* is not, the *`UACC or ID(*)`* selection only applies to UACC. When both or neither are selected, the selection applies to both UACC and ID(*).
Uncond. ID(*)	When this field is selected and *Universal access* is not, the *UACC or ID(*)* selection only applies to ID(*). When both or neither are selected, the selection applies to UACC and ID(*).
UACC or ID(*)	Show all general resource profiles with the specified UACC or an ACL entry with `ID(*)` that has the specified access level for the Operator specified in the entry field.
Show merged memberlist	Specify **1** for 'normal' output. Specify **2** to show a member overview first, followed by a profile overview at a deeper level. Specify **3** to show an overview of duplicate members, followed by a profile overview at a deeper level.

The merged `memberlist` option is not the way to find all profiles with members that cover a given resource. Use option **RA.3.7 Match** (see "RA.3.7 MATCH - Find profiles that cover a data set or resource" on page 216) instead.

A sample profile display is the following figure.

```
zSecure Admin General resource overview -------------------- Line 1 of 1
Command ===>                                                 Scroll===> CSR
Class %CIC*, containing CEDA                    2 Feb 1999 00:05
   Class    Profile key                                T UACC    Owner    S/F W
s_ GCICSTRN CIC410A.HANK                                 NONE___ C##BWTK_ __R _
****************************** BOTTOM OF DATA ********************************
```

The member list can be found on the detail display.

```
zSecure Admin General resource overview ------------------- Line 1 of 33
Command ===>                                                Scroll===> CSR
Class %CIC*, containing CEDA                  2 Feb 1999 00:05


  Identification                                                  DINO
  Class                          GCICSTRN
  Profile name                   CIC410A.HANK
  Type
  Volume serial list
_ Owner                          C##BWTK_                    WIGHT KENDALL
  Installation data              ____________________________________________
  Application data               ____________________________________________

  User     Access  ACL id   When               Name                InstData
_ C##BWTK  ALTER__ C##WTK_ ________ __________ WIGHT KENDALL

  Members
_ CEDA_____________________________________________________________________
_ CEMT_____________________________________________________________________

  Safeguards                           Other permissions
  User to notify of violation  ________ Allow all accesses    WARNING No_
  Audit access success/failures   R    Universal access authority    NONE___
  Global audit success/failures ___    Resource level                _0

  Mandatory Access Control             Statistics
  Security label                       Creation date                 10Apr98
  Security level
  Categories list

****************************** BOTTOM OF DATA ********************************
```

Additional selection - Access list

If the option **Access list** to display the second additional selection criteria panel has been selected, the panel shown in Figure 107 on page 159 is displayed.

Note:

See "Access list display modes - reference material" on page 30 for more information about the access list.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Selection
Command ===> ____________________________________________________________
Class %CIC*, containing CEDA
Specify additional selection criteria:
Find a combination of the following in the access list
# permits . . . . . __  ______              (operator: < <= > >= = <> ^= )
# conditional permits __  ______             (operator: < <= > >= = <> ^= )
Id on access list . ________                 (*, group or userid, or filter)
When resource . . . ________________         (resource name or filter)
Access level  . . . __  _   1. None       When class  . . _  1.  CONSOLE
                            2. Execute                      2.  APPCPORT
                            3. Read                         3.  TERMINAL
                            4. Update                       4.  JESINPUT
                            5. Control                      5.  SYSID
                            6. Alter                        6.  PROGRAM
                            7. Ignore                       7.  SERVAUTH
                                                            8.  CRITERIA
                                                            9.  Present
                                                            10. Ignore


Access list filtering
_   Only show matching ACL entries
```

Figure 107. Access list selection

Table 99 describes the supported selection criteria.

Table 99. Resource selection report - selection criteria

Criteria	Description
# permits	Specify the number of permits the profile should have.
# conditional permits	Specify the number of conditional permits the profile should have.
Id on access list	User or group on the access list (access that a user has through a group is *not* supported in this selection). You can use filters, consisting of % (one char), * (>1 char) and : (search).
When resource	You can select all resource profiles that have a conditional access list involving the string specified in the resource name for the condition. You can use the following filters in the ID specification: % for one character, * for one or more characters, and : for a substring scan.
Access level Operator	Use the operator to determine an access level present in the ACL. Use < and <= for selection less than or equal to the level, > or >= for high access, = for exact access, ¬= and <> for all but the specified access level.
Access level	Show all resource profiles with at least one permit with an access level satisfying the Access level Operator.
When class	Show all resource profiles with a conditional access involving the class indicated.
Only show matching ACL entries	Show a subset of the access list, consisting of the access list entries that match all of the criteria selected on this panel.

Line commands on a RESOURCE profile display

When you use **/** line command to ask which line commands are permitted, the following table is shown.

Table 100. Line commands on a RESOURCE profile display

Command	Meaning	Explanation
AC	Access Check for one `userid` or group	"RA.1 ACCESS - Access Check" on page 184
C	Copy general resource profile	"C - Copy" on page 55
CC	Copy to a different class	"CC - Copy to a different class" on page 56
D **DD**	Delete general resource profile, or delete a non-base segment,	"D - Delete" on page 58
E	Display event logging	"Reporting on general resource events (EV.R)" on page 567
K	Set or delete APPCLU session key	"K - Manage APPCLU and PTKDATA keys" on page 59
L	RACF `rlist` command	The output from the `rlist` command is presented in a browse panel.
MI	Manage information	"MI - Manage information" on page 61
MR	Manage CKGRACF authority requirements	"MR - CKGRACF mulitple authority requirement" on page 63
MU	Manage installation-defined USERDATA	"RA.3.9 USERDATA - User data management" on page 219
PE	Add or delete permit	"PE - Add or delete permit" on page 69
R **RR**	Recreate general resource profile	"R - Recreate a profile" on page 70
S	Show additional information	"S - Select" on page 72
SE	Show application segments	"SE - Show application segments" on page 72 and "Application segments" on page 161.
X **XX**	Exclude a profile from `FORALL` processing.	"X - Exclude profile line command" on page 74
Z **ZZ**	Select profile for `FORALL` processing.	"Z - Select a profile" on page 74

Add new general resource profile or segment

By pressing the push button *Add new general resource profile or segment* on the RA.R panel (put the cursor on it and press ENTER or put a / in front of it and press ENTER), you can request addition of a new, vanilla, general resource profile, or addition of an empty segment on the current system only. If you want to make a copy of an existing profile instead of building from scratch, or add a profile on another system through a batch job, type the profile name in the simple selection panel, display it, and then put the C (Copy) line command in front of it, instead of using this push button. The simple selection panel is described in "RA.R RESOURCE - General Resource profiles" on page 147.

When you press the *Add new general resource profile* or *segment* button the panel shown in Figure 108 on page 161 is displayed.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Add
Command ===>_____________________________________________________________

Class name  . . . . ________     (required)
Profile name  . . . ____________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
_____________________________ (required)
Owned by  . . . . . ________ (may also be set in the follow on update dialog)

/   Define new general resource profile

_   Add CDTINFO segment              _  Add PROXY segment
_   Add CFDEF segment                _  Add SESSION segment
_   Add DLFDATA segment              _  Add SIGVER segment
_   Add EIM segment                  _  Add STDATA segment
_   Add ICSF segment                 _  Add SVFMR segment
_   Add ICTX segment                 _  Add TME segment
_   Add KERB segment

Seclevel  . . . . .
Custom field type .    1. CHAR  2. NUM  3. FLAG  4. HEX
```

Figure 108. Add resource profile panel

When a new general resource profile is added, you specify a resource profile owner. The owner of the resource profile is saved to your ISPF profile and becomes the default profile owner for new profiles that you add. You can choose one of the following options: add a new profile, add a new segment to an existing profile, or add a new profile with a new segment. For the CFDEF segment, you are prompted to specify the Custom field type. For the SECLABEL class, you are prompted to specify the **Seclevel**. For the DIGTRING class, a panel displays which allows you to specify the Key ring name and Key ring owner. After you press Enter, the add command runs immediately on the system you are logged on to. The RACF command response is only shown if there is a nonzero return code. Next, the new profile, or segments are displayed with modifiable fields for further customization. The format of the display is the same as the detail display described in "Resource profile detail display" on page 152.

Application segments

When the *Show segments* option is selected, or the SE action command is used, application segments are displayed.

- "CDTINFO segment (CDT class)" on page 162
- "CFDEF segment (CFIELD class)" on page 163
- "CERTDATA segment (DIGTCERT class)" on page 164
- "DLFDATA segment (DLFCLASS class)" on page 165
- "EIM segment (LDAPBIND and FACILITY class)" on page 165
- "ICSF segment (CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY class)" on page 166
- "ICTX segment" on page 166
- "IDIDMAP Identity propagation mapping" on page 167
- "PROXY segment (LDAPBIND and FACILITY class)" on page 167
- "SESSION segment (APPCLU class)" on page 168
- "SSIGNON segment (PTKTDATA class)" on page 168
- "SIGVER segment (General Resource class)" on page 168
- "STDATA segment" on page 169

- "SVFMR segment (SYSMVIEW class)" on page 169
- "TME segment" on page 170
- "DIGTNMAP Certificate Filters" on page 170

CDTINFO segment (CDT class)

The CDTINFO segment for the CDT class is not supported under z/VM. In a RACF database that is shared between z/VM and z/OS, process these segments from the zSecure for z/OS product.

The CDTINFO segment is only valid for the CDT resource class. It is used to define classes in the dynamic CDT.

In this segment, the POSITs of related grouping and member classes are kept synchronized. When you overtype the POSIT of a grouping or member class with a value, an additional command is generated to also change the POSIT of the related class to the same value. You can still have grouping and member class pairs with unlike POSITs by setting the POSITs before creating the grouping and member relation.

Table 101. CDTINFO segment (CDT class)

Overview field	Detail field	Explanation
Pos	**POSIT (options set id)**	The options set id, a number in the range 0 to 1023 identifying a set of SETROPTS options that govern the activity of the user-defined class and all other classes having the same POSIT value.
Grouping	**Related grouping class**	For member classes, this field contains the name of the related grouping class
Members	**Related member class**	For grouping classes, this field contains the name of the related member class
RC	**Default not-found RC**	The default return code for the user-defined class
Oper	**OPERATIONS honored**	Whether OPERATIONS authority is honored for the user-defined class
UACC	**Default UACC**	The default universal access for the user-defined class.
Max	**Maximum length**	The maximum length of resource and profile names of the user-defined class.
MxE	**Maximum length with ENTITY**	The backward compatible maximum profile name length to be used with the ENTITY keyword form of the RACROUTE macro.
Scl	**SECLABELs required**	Whether SECLABELs are required for profiles in the user-defined class.
MAC	**MAC checking**	Which type of mandatory access control (MAC) processing is required for the user-defined class.
PrA	**Profile definition allowed**	Whether profiles are permitted in the user-defined class
GnA	**GENERIC/GENCMD status**	Whether SETROPTS GENERIC and GENCMD are permitted for the class

Table 101. CDTINFO segment (CDT class) (continued)

Overview field	Detail field	Explanation
Racl	**RACLIST status**	Whether profiles in the user-defined class can or cannot be SETROPTS RACLISTed, or are required to be RACLISTed.
Genl	**GENLIST status**	Whether the user-defined class can be GENLISTed
Sig	**Send ENF signal**	Whether an ENF signal must be sent when the user-defined class is being RACLISTed, NORACLISTed, or RACLIST REFRESHed.
Qu	**Generic scan limit (quals)**	The number of qualifiers at the start of the profile name that cannot be generic.
Lwr	**Profile names case sensitive**	Whether profile names in the user-defined class are kept as is or are converted to uppercase.
AN#S	**Syntax 1st character (raw)**	The syntax rules for the first character of a profile name in the user-defined class.
AN#S	**Syntax remainder (raw)**	The syntax rules for the remainder characters of a profile name in the user-defined class.

CFDEF segment (CFIELD class)

CFDEF segments can only be added at **CFIELD** profile creation time, and not later. When adding a **CFIELD** profile, a **CFDEF** segment and a Custom field data type are required.

Table 102. CFDEF segment (CFIELD class)

Overview field	Detail field	Explanation
RACF header	**Custom field listing header**	The heading to display in the output for the `LISTUSER` or `LISTGRP` command whenever the **CSDATA** segment is listed.
Type	**Custom field type**	The data type of the custom field. Valid data types are **CHAR**, **NUM**, **FLAG**, and **HEX**.
MaxL	**Custom field max length**	Maximum length of the value supported in `NUM`-type custom fields.
MinVal	**Custom field min value**	Minimum value supported in `NUM`-type custom fields.
MaxVal	**Custom field max value**	Maximum value supported in `NUM`-type custom fields.
CF1	**Custom field first char**	Syntax value of first character of `CHAR`-type fields. The default format prints a string such as `AN#S` where the letters indicate which character is permitted for a first character in `CHAR`-type fields. Possible values are: **A** for alphabetic **N** for nationals **#** for numerics **S** for all other characters

Table 102. CFDEF segment (CFIELD class) (continued)

Overview field	Detail field	Explanation
CF0	**Custom field other chars**	Syntax value of non-first characters of CHAR-type fields. The default format prints a string such as AN#S where the letters indicate which character is permitted for non-first characters in CHAR-type fields. Possible values are: **A** for alphabetic **N** for nationals **#** for numerics **S** for all other characters
Mix	**Custom field mixed chars**	Indicates whether mixed case characters are permitted in CHAR-type custom fields.
Help text	**Custom field help text**	Provides the help text for the custom field.

CERTDATA segment (DIGTCERT class)

The DIGTCERT CERTDATA segment contains digital certificate information.

Table 103. CERTDATA segment (DIGTCERT class)

Overview field	Detail field	Explanation
Profile key	**Ring profile name**	Profile key
#Cert	n/a	Number of certificates
Digital certificate labels	**Digital certificate labels**	Label of the certificate
User	**User**	Userid associated with the certificate
Tru	**Tru**	Whether the certificate is marked as trusted
Cert. sta	**Certificate startdate**	Certificate is valid from this date/time
Cert. end	**Certificate enddate**	Certificate is valid until this date/time
Subject's distinguished name	**Subject's distinguished name**	The user for whom the certificate was issued
Issuer's distinguished name	**Issuer's distinguished name**	Name of the issuer of the certificate
Serial number	**Serial number**	Serial number of the certificate
Key Type	**Private Key Type**	Type of private key
n/a	**Private Key Size**	Contains the size, in bits, of the private key
n/a	**Certificate lser**	Contains the last eight bytes of the last certificate that was signed with this key
n/a	**Certificate AltName email**	The email addresses of the subject as found in the subjectAltName extension of the certificate.
n/a	**Certificate AltName domain**	The domain names of the subject as found in the subjectAltName extension of the certificate.
n/a	**Certificate AltName IP addr**	The IP addresses of the subject as found in the subjectAltName extension of the certificate.
n/a	**Certificate AltName URI**	The universal resource identifiers of the subject as found in the subjectAltName extension of the certificate.

Table 103. CERTDATA segment (DIGTCERT class) (continued)

Overview field	Detail field	Explanation
n/a	**RACF format**	The keyUsage extension of the certificate as RACF would show it.
n/a	**X509 format**	The keyUsage extension of the certificate as defined by the X.509 standard.
n/a	**Ringname**	A list of full names (userid and keyringname) of the keyrings to which this digital certificate is connected.

CERTDATA segment (DIGTRING class)

The DIGTRING CERTDATA segment contains key ring information.

Table 104. CERTDATA segment (DIGTRING class)

Overview field	Detail field	Explanation
n/a	**Certificate Label**	The certificate label
n/a	**Usage**	The type of authorization the certificate is used for within the ring
n/a	**Dflt**	Indicator whether the certificate is the default certificate within the ring
n/a	**Certificate name**	The certificate name

DLFDATA segment (DLFCLASS class)

The DLFDATA segment is only valid for the DLFCLASS resource class. It specifies information that controls DLF objects in profiles in the DLFCLASS.

Table 105. DLFDATA segment (DLFCLASS class)

Overview field	Detail field	Explanation
Ret	**Retain flag byte**	Retain flag byte
Jobs	**Jobnames**	The number of job names on the overview , and job names on the detail level.

EIM segment (LDAPBIND and FACILITY class)

The EIM segment is used to store Enterprise Identity Manager information. The EIM segment is only valid for user IDs and the LDAPBIND and FACILITY resource classes. The three Registry fields are only valid on the IRR.PROXY.DEFAULTS profile in the FACILITY class.

Table 106. EIM segment (LDAPBIND and FACILITY class)

Overview field	Detail field	Explanation
EIM DomainDN	**EIM Domain Distinguished Name**	The distinguished name of the EIM domain.
Options	**EIM options**	Options that control the EIM configuration.
Local Registry	**Local RACF registry for EIM**	Name of the local RACF registry in EIM domains.
Kerberos Registry	**Kerberos registry for EIM**	Name of the Kerberos registry in the EIM domain that the system uses.
X509 Registry	**X509 registry for EIM**	Name of the X509 registry in the EIM domain that the system uses.

ICSF segment (CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY class)

The ICSF segment is used to store Integrated Cryptographic Service Facility attributes for the keys that are controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY.

Table 107. ICSF segment

Overview field	Detail field	Explanation
ASE	**Asym. key usage SECUREEXPORT**	This field specifies whether the asymmetric key controlled by general resources profiles in the ICSF related classes can be used to export or import symmetric keys.
AHS	**Asym. key usage HANDSHAKE**	This field specifies whether the asymmetric key controlled by general resources profiles in the ICSF related classes can be used to protect communication channels.
SKEx	**Symmetric key exportable by**	This field indicates whether the symmetric keys covered by general resources profiles in the ICSF related classes are permitted to be exported.
SCW	**Symmetric Key CPACF wrap**	This field indicates whether the symmetric keys covered by general resource profiles in the ICSF related classes are allowed to be rewrapped. **Note:** The key rewrapping operation requires the key to exist in plain text outside of the tamper-resistant hardware. If your site requires that a particular encrypted key never exists in plain text outside of *tamper-retamper-resistant*, then SYMCPACFWRAP=NO.
PKDSlbl	**PKDS labels**	This repeated group field specifies a list of the ICSF key labels pertaining to public keys which can be used to export the symmetric keys covered by general resources profiles in the ICSF related classes.
Klbl#	**# PKDS labels**	Count of PKDS labels.
Clbl	**Certificate labels**	This repeated group field specifies a list of digital certificate labels that can be used to export the symmetric keys controlled by general resources profiles in the ICSF related classes.
Clbl#	**# Certificate labels**	Count of certificate labels.

ICTX segment

The ICTX segment contains the configuration options that control the Identity Context Extension (ICTX). It is only valid for specific profiles in the LDAPBIND class.

Table 108. ICTX segment (LDAPBIND class)

Overview field	Detail field	Explanation
EIM	**ICTX uses EIM to map**	The ICTX identity cache uses Enterprise Identity Mapping (EIM) services to find a mapping to a z/OS user ID

Table 108. ICTX segment (LDAPBIND class) (continued)

Overview field	Detail field	Explanation
Use	**ICTX stores mapping**	The ICTX identity cache stores an identity mapping to a local z/OS user ID when provided by the application
Req	**ICTX requires mapping**	The ICTX identity cache requires identity mapping to a z/OS user ID
Time	**ICTX mapping timeout**	The time (in seconds) the ICTX identity cache stores an identity mapping

IDIDMAP Identity propagation mapping

The IDIDMAP display contains identity propagation mapping information.

Table 109. Identity propagation mapping - segment field descriptions

Overview field	Detail field	Explanation
#Maps	n/a	Number of identity mappings in the profile.
Profile key	**Profile name**	The profile name.
n/a	**Mapping label**	The labels for the identity mappings.
n/a	**Userid**	The userids to which the distributed identities are mapped.
n/a	**Registry**	The registries for the distributed identities mapped.

KERB segment (REALM class)

The KERB segment is only valid for the REALM resource class. It specifies z/OS SecureWay Server Network Authentication and Privacy Service information.

Table 110. KERB segment (REALM class) - Segment field descriptions

Overview field	Detail field	Explanation
Kerberos name	**Kerberos name**	Kerberos realm name.
MinTktLife	**Minimum ticket life**	Minimum ticket life granted for this realm in seconds.
DefTktLife	**Default ticket life**	Default ticket life granted for this realm in seconds.
MaxTktLife	**Maximum ticket life**	Maximum ticket life granted for this realm in seconds.
Encryption	**Supported encryption types**	Types of encryption that can be used for this realm.
Chk	**Validate address in tickets**	This field specifies whether the Kerberos server validates network addresses in encrypted tickets as part of ticket validation processing.

PROXY segment (LDAPBIND and FACILITY class)

The PROXY segment is only valid for the LDAPBIND and FACILITY classes. It is used to store LDAP proxy server information.

Table 111. PROXY segment (LDAPBIND and FACILITY class) - Segment field descriptions

Overview field	Detail field	Explanation
LDAP host	**LDAP host**	Host of LDAP server to contact

Table 111. PROXY segment (LDAPBIND and FACILITY class) - Segment field descriptions (continued)

Overview field	Detail field	Explanation
Bind name	**Bind distinguished name**	Bind information for LDAP server being contacted

SESSION segment (APPCLU class)

The SESSION segment is only valid for the APPCLU resource class. This segment is used to control the establishment of sessions between logical units under LU6.2.

In the detail view of the segment, the session entity names are listed, the numbers of failures, and the session key (if the input is not an UNLOAD).

No information is shown from the SSIGNON segment (classes PTKTDATA and KEYSMSTR) because this segment only contains an encryption key.

Table 112. SESSION segment (APPCLU class)

Overview field	Detail field	Explanation
ConvSecL	**Conversation security flags**	Conversation security flags
Loc	Lockout flag	Session flag byte
LastKeyChg	**Session key last change date**	Session key last change date
KyInt	**Session key days to expiry #**	Session key days to expiration
KyTry	**Invalid attempts #**	Invalid attempts
KyMax	**Failed tries before lockout #**	Invalid attempts before lockout
#Sent	n/a	Number of session entities
n/a	**Session key (clear text)**	Session key in clear text
n/a	**Hexadecimal session key**	Session key in hexadecimal

SSIGNON segment (PTKTDATA class)

The `SSIGNON` segment is only valid for the `PTKTDATA` class. It is used to store secured signon keys. Table 113 lists the fields available for this segment.

Table 113. SSIGNON segment (PTKDATA class)

Overview field	Detail field	Explanation
SIGVER	**SIGVER segment**	Indicates the start of the segment
SIGREQD	**Signature required**	Indicates whether the module must have a signature. Value can be `YES` or `NO`.

SIGVER segment (General Resource class)

The `SIGVER` segment is only valid for the General Resource class. This segment provides information about when a signature verification occurred and whether a load was failed because signature verification failed.

Table 114. SIGVER segment (General Resource class)

Overview field	Detail field	Explanation
SIGVER	**SIGVER segment**	Indicates the start of the segment
SIGREQD	**Signature required**	Indicates whether the module must have a signature. Value can be `YES` or `NO`.
FAILLOAD	**Loader SIGVER response**	The following values can be displayed. • ANYBAD • BADSIGONLY • Never
SIGAUDIT	**Signature auditing condition**	The value in this field indicates the conditions under which RACF records an SMF type 80 record with qualifier code 86. The following conditions are possible. • Bad signature • Any failing signature • Success • All • None

STDATA segment

The `STDATA` segment is only valid for the STARTED resource class. It is used to control security for started tasks.

Table 115. STDATA segment (STARTED class)

Overview field	Detail field	Explanation
Proc.Jobname	**Profile name**	Procedure/jobname combination
Userid	**Started task RACF userid**	RACF `userid` to be used for started procedure
Group	**Started task RACF group**	RACF group to be used for started procedure
Trus	**Trusted - allow any, log all**	Trusted - all is authorized and logged
Priv	**Privileged - allow any, nolog**	Privileged - all is authorized, do not log
Trac	**Trace - issue IRR812I**	Trace

SVFMR segment (SYSMVIEW class)

The `SVFMR` segment is only valid for the `SYSMVIEW` resource class. This segment defines profiles associated with a particular SystemView® for MVS application.

Table 116. SVFMR segment (SYSMVIEW class)

Overview field	Detail field	Explanation
SV script	**Default logon scripts**	Systemview default logon script
SV parms	**SVFMR parameter list**	Systemview parameter list

TME segment

The TME segment specifies that information in the Tivoli Security Management Application is to be added, changed, or deleted. TME role access specifications can be present for all resource classes, the other fields can only be present for the ROLE class.

Table 117. TME segment

Overview field	Detail field	Explanation
Roles	**TME role access specifications**	TME role access specifications (count on overview)
TME parent role	**TME parent role**	TME parent role
Child (count on overview)	**TME child roles**	TME child roles
Grps (count on overview)	**TME grps**	Groups referring to this ROLE
Rsrcs	**TME resource access specifications**	TME resource access specifications

DIGTNMAP Certificate Filters

The `DIGTNMAP BASE` segment contains Certificate Filters information.

Table 118. DIGTNMAP Certificate Filters

Overview field	Detail field	Explanation
n/a	**Certificate filter label**	List of labels describing the digital certificate filters that map to the key of this profile.
n/a	**Target ID of certificate fltr**	RACF `userid` that the digital certificate filters described in this profile map to
n/a	**Certificate filter is trusted**	The trusted status of the digital certificate filters that map to the key of this profile.
Certificate filter name	**Certificate filter name**	Issuer and subject name separated by ¢

Print format

Behind the *Print format* checkbox, a number of additional options can be chosen. The options behind and below only apply if this one has been selected. The print format is either tabular or form-oriented and can be selected by the *Full detail form* checkbox. The tabular form sacrifices some detail in favor of a readable printout. The print format can either use a print file width of at least 132, or forced into 79 columns through the *Narrow print* checkbox. The prints can be sorted in another way than by profile name through the *Sort differently* checkbox.

If *Sort differently* is selected, a sort order panel opens for each segment type to be included in the output data. If you specify both *Print ACL* and *Print names*, you can specify access list sort order on the right half of the base segment sort order panel. For example, for the base segment:

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Sort Order
Command ===>
All profiles
Specify up to 3 fields to act as          Select one field to act as
alternate base segment sort order         access list sort order
Select with 1 or / and optionally 2, 3    Select with 1 or /
_ Profile name (default)                  _ Decreasing access
_ Member class                            _ Userid
_ Profile type                            _ Id in access list
_ Installation data
_ Owner
_ Notify
1 Creation date (descending)
_ Universal access (descending)
_ Warning mode
_ Application data
_ Retention period (descending)
_ Level (descending)
_ By audit priority (descending)
```

In the sort order panels, one can specify up to three sort keys by entering *1*, *2*, or *3*in front of the sort criteria. If you want to sort on just one column, it is also possible to use a / instead of 1.

The following figure shows an example of wide tabular print output of general resource profile base segments, sorted by descending creation date:

```
RACF class FACILITY  - complex DINO     19Sep2000  18:34                                                                    page    1
Class FACILITY with owner SYSAUTH, sorted by creation

Profile key                              TW UACC    Owner    S/F SgF Created Notify  Lv Pri InstData
IRR.RADMIN.LISTUSER                         NONE    SYSAUTH    R     16Sep00          0
IRR.RADMIN.*                             G  NONE    SYSAUTH    R     16Sep00          0
$C2R.OPTION.RA.H                            READ    SYSAUTH    R     12Sep00          0
$C2R.OPTION.RA.H.3                          READ    SYSAUTH    R     12Sep00          0
$C2R.OPTION.CH.**                        G  NONE    SYSAUTH    R     25Aug00          0
$CNG.SCP.G.SYSAUTH.SYSPROG                  NONE    SYSAUTH          10Jun00          0
BPX.DEFAULT.USER                            NONE    SYSAUTH  R R      8Mar00          0    UNIX DEFAULT.USER MUST BE DISCRETE
     Appldata: C#UNIXU/C#UNIXG
IRR.DIGTCERT.ADD                            NONE    SYSAUTH  R R      3Mar00          0    ABILITY TO ADD A CERTIFICATE
```

The TW columns indicate Type and Warning status, respectively. For the meaning of the other columns see “Resource profile tabular display” on page 151. The classes always start on a new page.

When *Narrow print* is checked, the output is almost the same, except that installation data (if any) is on a separate line. This changes if *Print ACL* is also selected, the output is shown with each access level on a separate line:

```
RACF class FACILITY  Complex DINO     19Sep2000  18:38             page    1
Class FACILITY with owner SYSAUTH, sorted by creation

Profile key                           TW UACC    Owner    S/F SgF Created Notify Pri
IRR.RADMIN.LISTUSER                      NONE    SYSAUTH    R     16Sep00
IRR.RADMIN.*                          G  NONE    SYSAUTH    R     16Sep00
$C2R.OPTION.RA.H                         READ    SYSAUTH    R     12Sep00
     Read:     C##BMR2
$C2R.OPTION.RA.H.3                       READ    SYSAUTH    R     12Sep00
     None:     C##BPK2
$C2R.OPTION.CH.**                     G  NONE    SYSAUTH    R     25Aug00
     Read:     C##A C##B C##BQA C##QA SYSPROG
     None:     C##BMR1
$CNG.SCP.G.SYSAUTH.SYSPROG               NONE    SYSAUTH          10Jun00
     Update:   ADMIN SYSPROG
BPX.DEFAULT.USER                         NONE    SYSAUTH  R R      8Mar00
     Data:     UNIX DEFAULT.USER MUST BE DISCRETE
     Appldata: CRUNIXU/CRUNIXG
IRR.DIGTCERT.ADD                         NONE    SYSAUTH  R R      3Mar00
     Data:     ABILITY TO ADD A CERTIFICATE
     Read:     C##QARUN
```

When *Full detail form* is also selected, the profile forms are separated by dashed lines. When *Resolve to users* has been selected, the access list is resolved to user IDs (matrix). When *Show segments* and *All* has been selected, all segment information is

included on the form as shown in the following example.

```
Class STARTED  complex DINO     19Sep2000  18:50 BASE                page    1
Class STARTED with owner SYSAUTH


= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Identification
--------------
Class                        STARTED
Profile name                 PORT8010.*
Type                         GENERIC
Owner                        SYSAUTH                      AUTHORIZATION GROUP

Safeguards                           Other permissions
----------                           -----------------
User to notify of violation          Allow all accesses    WARNING No
Audit success access level           Universal access authority    NONE
Audit failures access level   READ    Resource level                 0

Mandatory Access Control             Statistics
------------------------             ----------
Security label                ........ Creation date                24Jan2000


STDATA segment
--------------
Started task RACF userid     C2RSRV#P Zsecur ADMIN WINDOWS C/RACF WIN SERVER P
Started task RACF group      C##BOMVS
Privileged - allow any, nolog No
Trusted - allow any, log all  No
Trace - issue IRR812I         No

= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

RA.S SETTINGS - SETROPTS and class settings

Menu option **RA.S** produces two reports, respectively showing the SETROPTS settings and class information from both the SETROPTS settings and the class descriptor table (CDT). They are designed to be a convenient way to change SETROPTS settings and class attributes.

```
zSecure Display Selection                          1 s elapsed, 0.6 s CPU
Command ===> ____________________________________________________ Scroll===> CSR
  Name     Summary Records Title
_ SETROPTS       1       1 RACF SETROPTS system settings
_ RACFCLAS     195     195 RACF class settings
****************************** Bottom of Data ********************************
```

The SETROPTS detail display is identical to “SETROPTS - RACF settings report” on page 266.

Class settings tabular display

The class settings display looks like this:

```
RACF class settings                                              Line 1 of 195
Command ===> ____________________________________________________ Scroll===> CSR
                                                  25 Apr 2005 00:07
   Class    Active Description
__ ACCTNUM  Active TSO account numbers__ ACICSPCT Active CICS program control table
__ AIMS     ______ IMS application group names (AGN)
__ ALCSAUTH ______ Supports the Airline Control System/MVS (ALCS/MVS) product
__ APPCLU   Active Verify ID of partner logical units during VTAM session estab
__ APPCPORT Active Controls which user IDs can access the system from a given L
__ APPCSERV Active Controls whether a program being run by user can act as a se
__ APPCSI   ______ Controls access to APPC side information files
__ APPCTP   ______ Controls the use of APPC transaction programs
__ APPL     Active Controls access to applications
```

By scrolling to the right, additional fields can be displayed. The following fields of interest are shown:

Class
Name of the class in the class descriptor table (CDT).

Active
RACF protection for this class is active (due to a SETROPTS CLASSACT command).

Description
A short explanation of the purpose of the class.

Generic
Generic profile checking for this class is active (due to a SETROPTS GENERIC command). This implies that generic command processing for this class is active.

GenCmd
Generic profile command processing for this class is active due to a SETROPTS GENCMD or a SETROPTS GENERIC command.

Audit
Command auditing for this class is active due to a `SETROPTS AUDIT` command.

Logopt
Auditing options for this class, due to a SETROPTS LOGOPTIONS command. The LOGOPT values can be *Always*, *Failure*, *Never*, *Profile* (determined by the logging options of the profile), and *Success*.

Global
Global Access Checking activity. This value is *Undefined* if Global Access checking is not permitted. It is *set* if Global Access checking is active, and *not set* if Global Access checking is inactive.

Raclist
This class has been RACLISTed which means that both generic and discrete profiles for this class are loaded into storage that is shared between address spaces. This processing occurs as a result of a `SETROPTS RACLIST(`*class*`)` command.

Genlist
This class has been GENLISTed as a result of a SETROPTS GENLIST command. A `GENLIST`ed class specifies that all generic profiles for the class are retained in-storage that is shared between address spaces.

Stats
Statistics are collected for this class (due to a SETROPTS STATISTICS command).

Complex
The name of the complex examined.

System
The name of the system examined.

RC
The default return code for this class. This code is returned when no matching profile can be found at a RACHECK. The result codes and their meanings are *0* (Grant access), *4* (Indeterminate: depends on resource manager) and *8* (Fail access).

Oper
This column contains the text OPER if the OPERATIONS attribute applies to this class. This means that all users with this attribute have access unless access is specifically denied.

Pos
This field contains the options set id, a number in the range *0* to *1023* identifying a set of SETROPTS options that govern the activity of this class and all other classes having the same POSIT value. Whenever a SETROPTS command is issued for any class with a specific POSIT value, it applies to all classes with that same POSIT.

Grouping
For member classes, this field contains the name of the related grouping class.

Members
For grouping classes, this field contains the name of the related member class.

Where
This field indicates profile residency. The possible WHERE values and their meanings are:

Genlist
Indicates profiles that have been GENLISTed as a result of a SETROPTS GENLIST command, which means that all generic profiles are retained in-storage shared between address spaces, but discrete profiles are not resident.

NoGenl
SETROPTS GENLIST is not permitted for this class. SETROPTS RACLIST is permitted but has not been specified.

NoList
SETROPTS RACLIST and SETROPTS GENLIST are not permitted for this class, usually because the applications automatically issue the RACLIST command.

NoRacl
SETROPTS RACLIST is not permitted for this class; SETROPTS GENLIST is, but has not been specified.

Nowhere
Profiles not permitted in this class.

RaclGbO
The profiles are resident only because they have been RACLISTed by an application via a RACROUTE macro with GLOBAL=YES specified.

Raclist
Profiles have been RACLISTed as a result of a SETROPTS RACLIST command, which means that they reside in a data space or in (E)CSA.

RaclReq
Profiles must reside in-storage if class is active.

(blank)
Class has not been RACLISTed or GENLISTed, but it would be permitted.

RFR
This flag indicates whether the current class is included in the SAF router table. See "ROUTER: SAF Router Table" on page 1250. If any *No* value occurs, there is a mismatch, and `RACROUTE` requests for this class return an *indeterminate* result (`RC=4`).

Max
This field contains the maximum length of profile names in this class. This value is a number in the range 1 to 246.

MxE
Maximum length for use with the ENTITY keyword of the RACROUTE macro.

UACC
This column contains the default universal access for profiles created in this class. This value is for setting the profile UACC during addition of a profile in this class if no UACC is specified on the command. UACC can have any of the following values: ALTER, CONTROL, UPDATE, READ, NONE, or ACEE. The last indication means that RACF uses the default UACC of the ACEE for the user.

User
The class is user-installed (as opposed to IBM-defined).

Id Generic class identifier. This is a number in the range 0 - 255 that is associated with the class name in the Class Descriptor Table and also stored in the `CLASTYPE` field of general resource profiles in the RACF database.

Org
The original order (entry number) of this class in the class descriptor table. The first entry in the table has `ORDER=1`.

NoProf
Profiles cannot be defined in this class.

RaclReq
A `RACLIST` is required for this class.

DataSpc
RACLISTed profiles for this class have been stored in a dataspace.

SeclReq
A security label is required for profiles in this class.

RvrsMAC
Reverse mandatory access checking is required.

EqualMac
Equal mandatory access checking is required.

RaclGlblOnly
The class is RACLISTed due to `RACROUTE GLOBAL=YES` only.

RaclOK
A `RACLIST` is permitted for this class.

GenlOK
A `GENLIST` is permitted for this class.

Signal
An `ENF` signal must be sent when the class is being RACLISTed, NORACLISTed, or RACLIST REFRESHed.

Qu
The number of qualifiers at the start of the profile name that cannot be generic.

Lowercase
The profile name can contain lowercase characters.

AN#S
This column occurs twice. The first one indicates whether the first character of the profile name can be alphabetical (*A*), a national character (*N*), numerical (*#*) or a special character (*S*). The second one applies to characters after the first one.

Same POSIT value
The classes that share the POSIT value with this class. Whenever a SETROPTS command is issued for any class with a specific POSITvalue, it applies to all classes with that value. This field lists all classes in the CDT, not only the active ones.

Class settings detail display

Select any class on the class settings table display to see the detail view. Selection can be done by putting the cursor on the first character of row selection field and pressing ENTER, or by explicitly typing S there and pressing ENTER.

A detail display is shown in Figure 109.

```
RACF class settings                                          Line 1 of 39
Command ===> ____________________________________________ Scroll===> CSR
                                        25 Apr 2005 00:07
  Class    Description
  ACICSPCT CICS program control table

  Class SETROPTS settings                                  DINO     DINO
  Protection active             Yes_____
  Command auditing active       Yes_____
  Logoptions                    Profile_
  GLOBAL (fast path) active     No______
  Generics checked              Yes_____ Generics can be activated     Yes
  Generic commands allowed      Yes_____
  Profiles RACLISTed            No       Profiles may be RACLISTed     No
  Profiles GENLISTed            No       Profiles may be GENLISTed     No
  Statistics collected          No______

  Profile syntax rules 1st     rest      Class properties
  Alphabetic allowed   Yes      Yes      Original order (class number)  40
  National allowed     Yes      Yes      Class identifier               37
  Numeric allowed      Yes      Yes      POSIT (options set id)          5
  Special allowed      Yes      Yes      Default UACC                   NONE
  Maximum length        13      Generic scan limit (quals)      0
  Maximum length with ENTITY    13      Installation-defined class     No
  Related grouping class        BCICSPCT Profiles names case sensitive No
  Related member class                   Default not-found RC           4

  Class activity options                 Profile residency options
  Profile definition forbidden  No       Profiles in dataspace          No
  OPERATIONS honored            No       RACLIST required               No
  Send ENF signal               No       RACLISTed by application only  No

  Mandatory access control properties
  SECLABEL required             No
  Reverse MAC checking          No
  Equal MAC checking            No

  Same POSIT value
  TCICSTRN GCICSTRN PCICSPSB QCICSPSB FCICSFCT HCICSFCT JCICSJCT KCICSJCT
  DCICSDCT ECICSDCT SCICSTST UCICSTST MCICSPPT NCICSPPT BCICSPCT CCICSCMD
  VCICSCMD
******************************* Bottom of Data ********************************
```

Figure 109. Class SETROPTS settings - Detail display

Line commands on the class settings display

When you use the / line command to ask which line commands are permitted, the following table is shown.

Command	Meaning	Explanation
C	Copy class setting	Copy a static or dynamic class descriptor table (CDT) entry. Commands to create a new CDT profile and CDTINFO segment are generated. Optionally, the following SETROPTS commands are generated: • SETROPTS CLASSACT • SETROPTS GENERIC • SETROPTS RACLIST or SETROPTS GENLIST is generated provided that the settings for the new class allow for SETROPTS RACLIST or SETROPTS GENLIST **Note:** SETROPTS RACLIST and SETROPTS GENLIST are mutually exclusive.
E	Display event logging	"Reporting on general resource events (EV.R)" on page 567
P	Display profiles	"RA.R RESOURCE - General Resource profiles" on page 147
R	Refresh class	Generate a SETROPTS REFRESH command
S	Show additional information	"S - Select" on page 72

RA.H HELPDESK - One-panel help desk options

The menu option **RA.H** (HELPDESK) can be used to perform the most common user administration tasks, and is especially designed for use by a decentralized or centralized help desk. If your installer chose to follow the suggestions in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*, it can also be started directly from ISPF by typing CKGHELP. The menu is displayed in Figure 110.

```
  Menu   Options   Info   Commands   Setup   Startpanel
--------------------------------------------------------------------------------
                          zSecure Suite - Helpdesk
Option  ===>

 1      List            List RACF profile information
 2      Password        Set a new password
 3      Default         Set the password to the user's default value
 4      Previous        Set the password to the previous value
 5      Resume          Resume a userid after too many password attempts
 6      Disable         Temporarily disable logon for a userid
 7      Enable          Allow user to logon after a Disable
 8      Set default     Define a default password for a userid

Userid  . . . . . ________     (type userid and press enter)
New password  . . .            (type new password)
Verify password . .            (type new password again)
Reason  . . . . . ____________________________________________________
Workflow option . . 1      1. Request  2. Withdraw  3. Approve  4. Deny
```

Figure 110. HELPDESK Menu

For a decentralized help desk, options 6 to 8 would typically be omitted from the panel by setting the access level to *NONE* on SAF resources CKR.OPTION.RA.H options 6 through 8. The setup of the help panel contents can be done using XFACILIT CKR.OPTION.RA.H profiles on a by-user or by-group basis.

Most of the options shown on this panel are familiar to a RACF administrator; the exception is the *default password*. The default password is an installation-defined option added by Security zSecure [1] An additional and inactive password is required that can only be set by selected administrators. This user must have the default password value. A larger group of administrators like the help desk can *apply* the default password. In this way, the administrators can reset the user password to a predetermined value, even if both the original and new passwords are not known to them.

Enter the **Userid** you want to act on, select an option, and enter any additional fields required for that option, then press ENTER.

The following options can be specified on the Help desk panel:

List
List RACF information about this user. For more information, see "LIST" on page 1515 for details.

Password
Set a new password for the user. Type the new password twice in the appropriate fields. The password must always be changed by the user at the next logon.

Default
Set the user password to the default value. If none has been defined yet, you are prompted for one.

Previous
Set the user password to the previous value.

Resume
Resume the user. This operation only succeeds if all `CKGRACF` schedules indicate that the user can have access to the system.

Disable
Change the user schedule so that the user cannot logon. This change can be accomplished by a hard revoke or soft revoke depending on the user authority. If the user has READ access to SYSADMIN, then that schedule name is used for a hard revoke. If the user has access to GRPADMIN but not SYSADMIN, then the GRPADMIN schedule name is used for a soft revoke. Otherwise, a default schedule accessible to the user is employed.

Enable
Change the schedule of the user so that he can logon as far as the help desk user is concerned. Note however that both schedule names GRPADMIN and SYSADMIN must agree before the user can actually work. That is, neither soft-revokes or hard-revokes have been requested.

Set Default
This sets the default password of a user for use by a help desk. This option should therefore not be available to that help desk.

The normal **Request type** for an administrator to use is `REQUEST`. If you are unauthorized to `REQUEST` the action, your installation might permit you to `ASK` for it. That is, add the action to the administrator queue for approval. If you specify `WITHDRAW`, you are attempting to undo a previous `ASK` or `REQUEST`. If an action has not been performed, you can `DENY` it to cancel the operation.

---

1. | Your local security policy might not permit the use of user fields in USER profiles. In this situation, default passwords are not available.

RA.Q QUICK ADMIN - Quick User Administration

The menu option **RA.Q** (QUICK ADMIN) can be used to perform the most common user administration tasks, and is especially designed for use by decentralized group administrators. If your installer chose to follow the suggestions in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*, it can also be started directly from ISPF by typing CKRQ. The menu is displayed in Figure 111.

```
Menu  Options  Info  Commands  Setup          StartPanel
------------------------------------------------------------------------------
                          zSecure Suite - RACF - Quick admin
Option ===> ____________________________________________________________

1    Password        Set new password for user
2    Resume          Make sure user can work
3    Display         List user definition
4    Modify          Change user definition
5    Connect         Add group to a user
6    Add user        Create new userid from scratch
7    Add user copy   Create new userid like existing model
8    Phrase          Set new password phrase for user

Userid  . . . . . . . . ________  (type userid and press enter)
New password  . . . . .           (type new password, option 1 only)
Verify password . . . .           (type new password again, option 1 only)
Group . . . . . . . . . ________  (type connect group, option 5 only)
```

Figure 111. QUICK ADMIN Menu

Enter the **Userid** you want to act on, select an option, and enter any additional fields required for that option, then press ENTER.

The following options can be specified on the panel:

Password
Set a new password for the user. Type the new password twice in the appropriate fields. The password must always be changed by the user at the next logon.

Resume
Resume the user in RACF. This field does not affect any CKGRACF schedules.

Display
List RACF information about this user which includes the following basic information:

- Identification: name, owner, default group, installation data.
- System access: Current revoke status and active status.
- Statistics: Creation date, last logon (connect) date, last use date.
- All the Connects with each the installation data for each group.

Modify
Change RACF information for this user. This command provides modifiable fields for basic user information: User name, owner, default group, current revoke status, and Connect list. In addition, this command lists each Connect entry with a line command field for copying or deleting the entry.

Connect
Connect the user to the group. This command provides a fast way to create a basic Connect that has USE authority and no other attributes.

Add user
Create a new user. This option opens a data entry panel requesting a name for the user ID (required), a default connect group (required), the owner, a new password (twice), and optionally installation data and a password phrase. When NLS options remove option **RA.Q.8** Phrase from the **RA.Q** display, the password phrase is also removed from this panel. See also the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Add user copy
Create a new user almost exactly like an existing model user profile. This option opens a data entry panel requesting a different name for the user ID (required), the `userid` for the model user profile, the owner, a new password (required, twice), and optionally different owner, default group, and installation data.

Note: Protected user IDs cannot be created with this function. To create these IDs, use the **Protected** option of the **C** (copy) line command available from option **RA.U**.

Phrase
Set a new password phrase or clear the password phrase for the user.

RA.W Windows - zSecure Visual administration

Use the menu option **RA.W** for selecting users or groups that are marked for deletion by zSecure Visual administrators. The option is only available when the zSecure Visual product is installed and not disabled. The panel shown for this function depends on the product combination and `IFAPRD`*xx*. That is, when only zSecure Visual is installed the panel content is different than it is when both zSecure Visual and zSecure Admin are both installed and active.

If your IBM Security zSecure Admin is installed and active, the **RA.W** function shows the list of users or groups that are marked for deletion. You can selectively confirm or cancel the delete operation for each of these users or groups. Without the IBM Security zSecure Admin component, the `RA.W` function only generates the commands to remove the users or groups. You can still edit the generated commands before you run them.

When both zSecure Visual and zSecure Admin are installed, the following panel is shown:

```
 Menu  Options  Info  Commands  Setup          StartPanel
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - Windows
Command ===> ____________________________________________________________

This panel allows you to select users or groups that are marked for deletion
by zSecure Visual administrators

Show userids that are marked for deletion
Userid  . . . . . . . . ________  (user profile key or filter)

Show groups that are marked for deletion
Group . . . . . . . . . ________  (group profile key or filter)
```

Figure 112. Visual selection panel with zSecure Admin

You can specify the following information on this panel:

Userid
Enter the user ID you want to select. To select more than one user ID, you can specify a filter using the following wildcard values: % to represent one character, or * to represent one or more characters.

The specified value provides the search criteria for selecting user IDs marked for deletion by zSecure Visual administrators. These user IDs are selected by the following command: CKGSCHED=$DELETE.

Userid is mutually exclusive with the Group field.

Group
Enter the group you want to select. To select more than one user ID, you can specify a filter using the following wildcard values: % to represent one character, or * to represent one or more characters.

TThe specified value provides the search criteria for selecting groups marked for deletion by zSecure Visual administrators. These groups are selected by the following command: USRNM=CNGDELET.

Group is mutually exclusive with the **Userid** field.

After you specify the search criteria and press Enter, the panel shown in Figure 113 opens to see the list of users or groups marked for deletion.

```
zSecure All users marked for deletion overview              Line 1 of 4
Command ===> _____________________________________________ Scroll===> PAGE
Type D in front of each user to delete          21 Jun 2005 11:04
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ C##QA001 DINO     QA SUBJECT 001______ C##QA___ C##QA___ ____ ___       X   2
__ C##QA002 DINO     QA SUBJECT DUAL AUTH C##QA___ C##QA___ ____ ___ g     X   2
__ C##QA003 DINO     QA SUBJECT 003______ C##QA___ C##QA___ ____ ___       X   1
__ C##QA004 DINO     QA SUBJECT 004______ C##QA___ C##QA___ RI__ ___       X   1
****************************** BOTTOM OF DATA ********************************
```

Figure 113. Visual users marked for deletion overview

For a description of the fields displayed, see "User profile tabular display" on page 89.

On this display, typing D in front of a user ID or group ID, depending on the profile option you selected, opens a panel like the one described under option D in "Line commands" on page 54. From that panel, you can generate the commands to remove the user or group. You can also decline the removal of a user ID or group ID by zooming in to the detail display using the S line command) and, on the detail display, deleting the $DELETE schedule by typing D in front of it.

When only zSecure Visual is installed, the following panel is displayed:

```
  Menu  Options  Info  Commands  Setup          StartPanel
--------------------------------------------------------------------------------
                        zSecure Visual Server Admin - RACF - Windows
Command ===> ____________________________________________________________

This panel permits you to select users or groups that are marked for deletion
by zSecure Visual administrators

Generate remove commands for userids that are marked for deletion
Userid  . . . . . . . . C#MXC02_  (user profile key or filter)

Generate remove commands for groups that are marked for deletion
Group . . . . . . . . . ________  (group profile key or filter)
Specify resources to delete
/  Data set and id-specific profiles
Only if previous option selected:
_  RACFVARS profiles and members
/  Data sets and their catalog entries
_  Incl. catalog entries without data sets
_  Incl. uncataloged data sets
Change USERID in Notify fields to   ________  (default is NONOTIFY)
New Owner for non-dataset profiles  ________  (default is SYS1)
```

Figure 114. zSecure Visual selection panel without zSecure Admin

The following fields can be specified on the panel:

Userid
Enter the user ID you want to select. To select more than one user ID, you can specify a filter using the following wildcard values: `%` to represent one character, or `*` to represent one or more characters.

The specified value provides the search criteria for selecting user IDs marked for deletion by zSecure Visual administrators. These user IDs are selected by the following command: CKGSCHED=$DELETE.

`Userid` is mutually exclusive with the `Group` field.

Group
Enter the group you want to select. To select more than one user ID, you can specify a filter using the following wildcard values: `%` to represent one character, or `*` to represent one or more characters.

TThe specified value provides the search criteria for selecting groups marked for deletion by zSecure Visual administrators. These groups are selected by the following command: USRNM=CNGDELET.

Group is mutually exclusive with the **Userid** field.

Data set and id-specific profiles
Selecting this option generates RACF commands to delete any RACF dataset profile which starts with the group ID or user ID. Profiles in other classes which have the group ID or user ID in certain predefined qualifiers are also deleted. If no matching profiles exist, then the delete command fails.

RACFVARS profiles and members
This option controls whether apparent occurrences of user IDs and group IDs in the key or member list of profiles in this class should be considered meaningful, and hence imply (partial) deletion.

Incl. catalog entries without data sets and Incl. uncataloged data sets
You can include or exclude catalog entries without data sets and uncataloged data sets as required. If you receive any inconsistency warnings, investigate them because they can indicate that residues remain, especially for VSAM errors.

Data sets and their catalog entries
This option controls if the data sets and catalog entries implied are deleted too. The ones protected by a profile to be deleted, or unprotected but with an HLQ matching a deleted id are implied.

Change USERID in Notify fields to
This option permits you to enter a USERID to get RACF notifications which would have previously been sent to one of the USERIDS to be deleted.

New Owner for non-dataset profiles
If you delete a user ID or a group ID which was the RACF owner of any profiles, the ownership of these profiles is changed based on the following rules:

- For group data sets, the ownership is changed to the high-level qualifier (HLQ).
- For connect profiles, the ownership is changed to the group and owner specified in this field.

  If you do not specify an owner, ownership defaults to *SYS1*.

After pressing enter, REMOVE commands are generated for the user IDs or groups selected. These are displayed in an ISPF EDIT session:

```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
-------------------------------------------------------------------------------
EDIT       C#MBMR4.C2R1EF2A.CKR2PASS                     Columns 00001 00072
Command ===>                                               Scroll ===> PAGE
Press PF3, enter R at the cursor location, press ENTER to run these commands
000001  suppress  deldsd
000002  remove user=C#MCX02   /* TEST USER, NO TSO                          *
****** **************************** Bottom of Data ****************************
```

Figure 115. Visual CKR2PASS file

After verifying the commands, press PF3 to return to the results panel and enter an **R** at the cursor location. The remove commands are run, and TSO commands are generated to delete the users or groups. These are displayed in an ISPF EDIT session:

```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
-------------------------------------------------------------------------------
EDIT       C#MBMR4.C2R1EF2A.CKRCMD                       Columns 00001 00072
Command ===>                                               Scroll ===> PAGE
Press PF3, enter R at the cursor location, press ENTER to run these commands
000001          /* CKRCMD file CKR1CMD complex DINO generated  8 Feb 2005 10:27
000002          /* Commands generated by (RE)MOVE USER/GROUP */
000003         remove C#MCX02  group(C#MCXDEL)
000004         remove CRMCX02  group(C#MCXGRP)
000005         raclink id(C#MCX02 ) undefine(DINO.C#MCX01)
000006         deluser C#MCX02  /* dfltgrp=C#MC     */
****** **************************** Bottom of Data ****************************
```

Figure 116. Visual CKRCMD file

Again, after verifying the commands, press PF3 to return to the results panel and enter an **R** at the cursor location to run the TSO commands. The result of the command execution is displayed in an ISPF BROWSE session.

RA.1 ACCESS - Access Check

Use the **RA.1 Access** option to test the access of a user or group on a dataset or general resource profile. For the DATASET class you can also specify a data set name, to see the access level on the profile covering this data set.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Access Check
Command ===>

Id  . . . . . . . . C##BJTI_

 Specify profile for Access Check
  Class  . . . . . . DATASET_  (DATASET or class)
  Profile  . . . . . SYS1.IPLPARM_____________________________ (EGN mask)
```

Figure 117. Access check panel

This example queries what access the user ID C##BJTI has on the resource SYS1.IPLPARM in the DATASET class. This query generates the CKGRACF command shown on the confirmation panel. The confirmation panel shown in Figure 118 is shown based on the Confirmation setting on the SETUP CONFIRM panel.

```
                          zSecure Suite - Confirm CKGRACF command
Command ===> ____________________________________________________________________
Confirm or edit the following CKGRACF command
ACCESS C##BJTI DATASET SYS1.IPLPARM









Command execution . 2  1. EXECUTE RACF command
                       2. EXECUTE CKGRACF command (allows use of Reason)
                       3. ASK administrator to execute CKGRACF command
                       4. REQUEST CKGRACF command for later execution
                       5. WITHDRAW CKGRACF command







Reason . . . . . . .  ____________________________________________________

Press ENTER to continue or END to cancel the CKGRACF command
```

Figure 118. Access command confirmation panel

After pressing **Enter**, the command is run regardless of the SETUP CONFIRM **Action on command** setting. The result of the command is shown in a browse panel. In this example, a fully qualified data set name was used which results in a panel showing the access to the profile covering this data set.

```
 Menu  Utilities  Compilers  Help
------------------------------------------------------------------------------
 BROWSE    MYTSOID.C2R1EF2A.CKRTSPRT                 Line 00000000 Col 001 080
 Command ===>                                          Scroll ===> CSR
******************************** Top of Data ********************************
CKGRACF  ACCESS C##BJTI DATASET SYS1.IPLPARM
CKG582I 00 C##BJTI has READ access to DATASET SYS1.IPLPARM
profile DATASET SYS1.*.**
******************************** Bottom of Data ********************************
```

Figure 119. Access check output file

RA.2 QUEUED - Queued commands

Queued commands are CKGRACF commands that are either subject to multiple-authority or are timed or temporary. CKGRACF is the APF-authorized component of IBM Security zSecure Admin. This function provides support for managing the following command-related services:

- Group administration based on function-specific profiles.
- Manage the *multiple-authority* option.
- Delay execution of a command until a future date using timed commands.
- Request temporary commands. For example, create a command that reverses the effects of a command at some later date.

Use Option **RA.2** to find and review queued commands, and then act on them. If your installation does not use these functions, you can skip this queued commands topic.

Multiple Authority

The multiple-authority requirement of a CKGRACF command can be SINGLE, DUAL or TRIPLE; if it is DUAL or TRIPLE, this means that after the initial REQUEST by an authorized user, it is queued for approval by one or two other authorized users.

The multiple-authority requirement of such a command is determined by the multiple-authority setting in the target profile or, if it contains none, the installation-wide default.

Unauthorized users might be permitted to ASK for (as opposed to REQUEST) a command by the installation. This always queues the command for approval. (However, ASK is not supported for TRIPLE authority requests.)

The Approval Queue

The approval queue contains requests that are not yet fully authorized. When you ASK or REQUEST a command, and it is queued for approval, the status asked (A) or requested (R) is assigned. At this stage the requestor can WITHDRAW the command which removes it from the approval queue and generates an audit trail entry. An authorized user who has not yet authorized the command can APPROVE it. Depending on the applicable multiple-authority setting, the command can now either be fully authorized or require further authorization.

If the command is fully authorized, it is removed from the approval queue. If it is a timed command specified to run at a future date, it is added to the execution queue. An Immediate command is run and an audit trail entry is generated.

If you APPROVE a command that has the multiple-authority setting, the command is moved to the next approval stage. For example, if the command is a TRIPLE authority command, the first approval is followed by a second approval request (SR) stage, and then a third approval *Request* stage.

An authorized user who has not yet taken part in authorizing the command can DENY it. If a command is denied, it is removed from the approval queue and an audit trail entry is generated. If a command has been queued for approval, but no action is taken within a reasonable time, the command expires. It is removed from the approval queue and an audit trail entry is generated. To keep a request longer than usual, an authorized user can HOLD it. Held commands then move to the second held (SH) or complete held (CH) stage.

The Execution Queue

The execution queue contains timed commands that have been approved, but for which the requested start date has not been reached yet. They have the status pending (P).

A timed command is a command that contains an "AT *date*" qualifier. It can be either permanent or temporary, depending whether it also contains a "FOR *days*" or "UNTIL *date*" clause.

When the start date is reached, the command is removed from the queue and run, and an audit trail entry is generated. If the command is a temporary one, a permanent timed command is queued to the execution queue with the end date of the original one as its start date to reverse its effect in time. Such a reverse has the pending reverse (PR) status.

Reviewing queued commands

Selecting **RA.2** Queued brings you to the panel shown in Figure 120.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Queued
Command ===>

Show only profiles that fit all of the following criteria:
Class name  . . . . ________     (class or filter)
Profile pattern . . SYSS.**_____________________________________ (EGN mask)
Complex . . . . . . ________     (complex name or filter)

Show only profiles with
 1  1. Queued commands requiring action
    2. Commands in the execution queue
    3. Withdrawn, denied or expired commands
    4. Any queued commands

Enter "/" to select option(s)
 _  Show all queued commands within selected profiles
```

Figure 120. Queued commands selection panel

The Class name, Profile pattern, and Complex field can be specified to limit the search for queued commands. You can specify a search filter using the generic characters % and *. Use the next option to specify selection criteria for the queued commands you are interested in. You can select using the following command type criteria:

- Outstanding command requests.
- Commands authorized to run at future date.

- Commands that have been denied.
- All queued commands, including those commands that have been denied.

Most of the selection criterion for commands also determines what commands are shown for each selected profile. However, you can choose to see all the commands within the selected profiles by selecting the option for all queued commands.

Figure 121 shows a sample display panel.

```
zSecure Admin PROFILE display                          Line 1 of 1
Command ===>                                           Scroll===> CSR
                                          16 Dec 1998 00:05
   Class    Profile key                       Expires LastReq LastChg
s_ USER     C##QA048 NOMEN NESCIO              22Dec11 15Dec11 15Dec11
****************************** BOTTOM OF DATA ********************************
```

Figure 121. Queued commands profile display

Each line lists the profile class, the profile key, the first date a queued command expires, the latest date a command was requested, and the latest date a command was changed including requests. For User profiles the user name is shown as well, while for Group profiles the installation data is included. You can sort the display on any column using the SORT command. For example, to sort commands based on the date before which they must be acted upon, type `SORT 'Expires'` behind the **Command ==>** prompt.

After a profile has been selected, the following detail panel is shown.

```
zSecure Admin PROFILE display                                  Line 1 of 8
Command ===>                                                     Scroll===> CSR
                                                 16 Dec 1998 00:05
   Class    Profile key                                 Expires LastReq LastChg
   USER     C##QA048 NOMEN NESCIO                       22Dec98 15Dec98 15Dec98
  CKGRACF authority requirement
_ Authority setting DUAL set by C##QARUN at 15 Dec 1998 18:39

  Commands requiring administrator action
_ Queued command (R): USER C##QA048 PWDEFAULT PASSWORD; request by C##QARUN at
  Inactive commands
_ Queued command (E): USER C##QA048 SCHEDULE HELPDESK DISABLE (30Aug1998:31Aug2
  Commands that have been executed
_ Queued command (CA): USER C##QA048 PWRESET; request by C##QARUN at 15 Dec 1998
****************************** BOTTOM OF DATA ********************************
```

Figure 122. Queued commands detail display

The detail panel shows the multiple-authority requirement, if set, and the queued commands. The status of the queued command is indicated between parentheses.

Table 119 lists the possible status values for a queued command. Depending on the command status, you have options to run different line commands. The following table indicates which line commands are available based on the status value of the queued command.

Table 119. Queued commands - status types

Abbreviation	Command status
(A)	Asked . This command is waiting to be approved or denied. The available line commands are **A**, **C**, **D**, **H**, **I**, **R**, and **S**.

Table 119. Queued commands - status types (continued)

Abbreviation	Command status
(CA)	Complete approve. This command has been approved and run. The actions permitted are **C**, **I**, **R**, and **S**.
(CD)	Complete deny. This command has been denied and cannot be run. The actions permitted are **C**, **I**, **R**, and **S**.
(CH)	Complete hold . The command is on hold. It can either be approved or denied. The actions permitted are **A**, **C**, **D**, **H**, **I**, **R**, and **S**.
(E)	Expired This. Command can no longer be completed. The actions permitted are **C**, **I**, **R**, and **S**.
(P)	Pending This. Command has been approved; it is now waiting for its execution date. The actions permitted are **C**, **D**, **I**, **R**, and **S**.
(PR)	Pending reverse . Command is the reverse of a temporary command that has been run. It is waiting for its execution date–that is, the end date for the temporary command. The actions permitted are **C**, **I**, **R**, and **S**.
(R)	Requested. Command is waiting to be approved or denied. The actions permitted are A, C, D, H, I, R, and S.
(SA)	Second approve . This command has been approved, but must be approved again (complete approve) before being run. The actions permitted are **A**, **C**, **D**, **H**, **I**, **R**, and **S**.
(SD)	Second deny . This command has been denied, and the command cannot be run. The actions permitted are **C**, **I**, **R**, and **S**.
(SH)	Second hold . This command is on hold and can be approved to pass on to the *complete* stage or denied. The actions permitted are **A**, **C**, **D**, **H**, **I**, **R**, and **S**.
(W)	Withdrawn . This command request has been withdrawn, and cannot be run. The actions permitted are **C**, **I**, **R**, and **S**.
(X)	Executed . This command has been approved and run. The actions permitted are **C**, **I**, **R**, and **S**.

The following action characters (line commands) can be used to work with the queued commands.

Table 120. Queued commands - available line commands

Action character	Effect
A	Approve a queued command.
C	Display a filled-in REQUEST panel to request a new command.
D	Deny or withdraw the queued command.
H	Hold a queued command.
I	Display an empty REQUEST panel to request a new command.

Table 120. Queued commands - available line commands (continued)

Action character	Effect
R	Create a copy of the queued command (repeat the request).
S	Display the queued command in more detail.

When you run the **C** line command, a completed REQUEST panel is shown. The panel shown depends on the type of queued command that is repeated. If the queued command pertains to schedules, you get a dedicated panel. If it is a PERMIT, CONNECT or REMOVE command, you get a general CKGRACF CMD panel. Another panel is shown for requests related to passwords and soft-resumes.

When you issue the **I** line command on a group profile display, you are prompted with a dedicated Connect/Remove panel. For a DATASET profile, the PERMIT panel opens. For a user profile, you are prompted to specify whether you want to issue a SCHEDULE command or a command related to passwords.

Figure 123 shows the Request a password panel.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Admin - Request a command
Command ===> ________________________________________________________________

Userid  . . . . . . . ADGRANT_

Select action:                                        Options
6  1. New password         ==>           ==>          /  Password expired
   2. Interval             ==> ___                    /  Resume userid
   3. DEFAULT password                                _  Ignore pw history
   4. PREVIOUS password                               _  Bypass pw rules
   5. RANDOM password                                 _  Bypass pw exits
   6. Resume only
   7. Make Protected

Request type  . . . . _  A(sk), R(equest) or W(ithdraw)
```

Figure 123. Request a command panel - password commands

Userid
The user you want to request a command for. Specify a valid user ID, without filter patterns.

Select action
Choose one of the numbered actions.

1. New password
This option can be used to reset the password to a new value. When this action is selected, you have to specify the new password twice.

2. Interval
This option can be used to set the password interval. Enter 0-254 for a specific password interval or N for no interval. When no value is entered the SETROPTS password interval setting is used.

3. DEFAULT password
This option can be used to set the password to a default value.

4. PREVIOUS password
This option can be used to set the password to the previous value.

5. RANDOM password
This option can be used to set the password to a random value.

6. Resume only
This option can be used to resume the user ID.

7. Make Protected
This option can be used to make this user ID protected from revoke due to too many password attempts.

Options
Each of these options can be selected by placing a '/' in front of them.

Password expired
Specifies that you want the user to change the password at the next login.

Resume userid
Specifies the user ID to be resumed. This option can be specified without resetting the password.

Ignore pw history
This option can be used to disable the history check performed by CKGRACF when a password is set.

Bypass pw rules
This option can be used to disable the password rule check performed by CKGRACF when a password is set.

Bypass pw exits
This option can be used to disable the ICHPWX01 exit call from CKGRACF when a password is set.

Request type
A CKGRACF parameter for multiple-authority, normally set to REQUEST. In some installations, end users might be permitted to ASK for permissions. A request that is not authorized to be run immediately shows up in the administrator approval queue for review. To retract a request in the approval queue (either due to ASK or because of a DUAL or TRIPLE authority requirement) specify WITHDRAW.

The Manage User schedules panel can be used to specify scheduled enabled or disabled periods; to list all scheduled revoke/resume events; or to wipe scheduled events. The panel is displayed in Figure 124 on page 191. Use option **1** to list all CKGRACF settings for the user ID, including all scheduled events and the overall schedule. Use the other options to add or wipe scheduled events. Use the **MS** line command to work with scheduled events.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure - Manage User schedules
Option ===> ____________________________________________________________

1  List         List schedules for this userid
2  Enable       Specify date(s) when user should be able to logon
3  Disable      Specify date(s) when user should not be able to log on
4  Wipe         Remove scheduled events at specified date(s)

Userid  . . . . . . . C##BSG1
Schedule  . . . . . . ________

Start date  . . . . . __________  End date  . . . . . . __________
                                  Number of days  . . . ___

Enter reason below
____________________________________________________________________________
```

Figure 124. Manage User Schedules

Schedule
The schedule name. If you use any of the options **2** to **4**, the schedule name is required.

Start date
The start date, required for options **2** to **4**. A date is specified in the format 01JAN1995.

End date
Optional end date. If specified, the scheduled enabled or disabled period extends from the start date up to (and including) the end date. Cannot be combined with 'Number of days'.

Number of days
Optional number of days an enabled/disabled period lasts. Cannot be combined with 'End date'.

Reason
Optional reason for the scheduled action (options **2** and **3**) or optional wipe reason (option **4**).

A queued command can contain both SCHEDULE and PASSWORD parameters. If you repeat such an entry, both panels are presented. When you build a command string for a single user, you cannot alter the **Userid** on the second panel if you already specified a command on the first panel. To avoid confusion you are not permitted to alter the **Request type** on the second panel in that case either.

Figure 125 shows the dedicated REQUEST CONNECT/REMOVE panel.

```
                      zSecure Suite - Request connect/remove
Command ===> ____________________________________________________________

Specify Group and User:
Group          ===> SYS1____         Connect/Remove ===> CONNECT
Userid         ===> ________

Request parameters:
Start date     ===> _________        End date       ===> _________
Number of days ===> ___

Request type   ===> R                A(sk), R(equest) or W(ithdraw)
```

Figure 125. Request connect/remove panel

Group
The group to connect to or remove from.

Connect/Remove
Indicates if the request is for connecting the user to the group or removing the connection.

Userid
The user to connect or remove from the Group.

Start date
The start date, required for options **2** to **4**. A date is specified in the format 01JAN1995.

End date
Optional end date. If specified, the scheduled enabled or disabled period extends from the start date up to (and including) the end date. Cannot be combined with 'Number of days'.

Number of days
Optional number of days an enabled/disabled period lasts. Cannot be combined with 'End date'.

Figure 126 shows the dedicated REQUEST PERMIT panel.

```
                        zSecure Suite - Request permit
Command ===> ____________________________________________________________

Specify profile:
Class . . . . . . . DATASET
Profile . . . . . . 'C##BFK1.CNRACF%.CKRCMD'
Generic . . . . . . ___        (Yes for fully qualified generic, default No)

User or group on access list to process (specify new access or enter Delete):
User/group  . . . . C##B____
Access  . . . . . . ALTER__    (Delete/None/Execute/Read/Update/Control/Alter)

Request parameters:
Start date  . . . . 01JAN2005_       End date . . . . .  __________
                                     Number of days . .  30_

Request type  . . . R                A(sk), R(equest) or W(ithdraw)
```

Figure 126. Request permit panel

Class
The class of the profile you want to grant a permit to or revoke a permit from.

Profile
The profile you want to grant a permit to or revoke a permit from.

Generic
If the profile is a fully qualified generic, which is a generic profile that contains no generic characters, specify YES in this field. In all other cases, you can leave this field blank.

User/group
Specify the user or group id to grant a permit to the profile to or take away a permit to the profile from this field.

Access
Specify the desired level of access in this field. To remove an existing permit rather than grant a new one, specify DELETE in this field.

Start date
The start date, required for options **2** to **4**. A date is specified in the format 01JAN1995.

End date
Optional end date. If specified, the scheduled enabled or disabled period extends from the start date up to (and including) the end date. Cannot be combined with 'Number of days'.

Number of days
Optional number of days an enabled/disabled period lasts. Cannot be combined with 'End date'.

Figure 127 shows the generic REQUEST CMD panel.

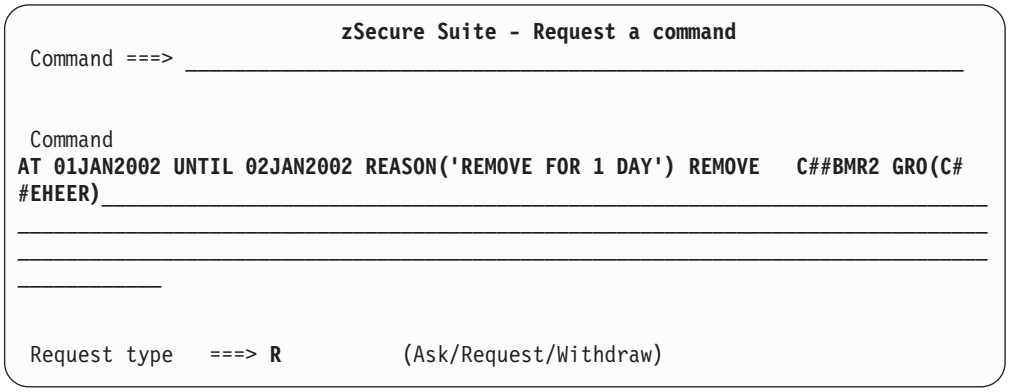


Figure 127. Request a command panel

Apart from the **Request type**, specify the entire CKGRACF CMD. You can enter fairly long commands; in a display of this width you can use in fact several lines, not just one.

RA.3 Reports - Reports with profiles and resources

Option **RA.3** Reports offers a number of special reports.

```
 Menu  Options  Info  Commands  Setup          StartPanel
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Reports
Option  ===>

1    Profiles        Any profiles fitting mask/qualifier with their data sets
2    Non redundant   Data set profiles different from less specific profiles
3    Redundant       All data set profiles, mark if non-redundant (as in 2)
4    Permit/scope    User/group on access list, or access by any means
5    Out of group    Group data sets accessible to users outside the group
6    Non default     Data sets with more in access list than 'owner has alter'
7    Match           Find profiles that cover a data set or resource
8    Group tree      Group tree display
9    USERDATA        Display and action on profiles with USERDATA
A    Tapevol         Tapevol profile overview
B    RACFvars        RACF variable profiles
C    APPL            Application profiles
D    JES/328X        Jes/328X definitions and log data sets
E    SDSF            SDSF command and display authorities
F    JES2            Access to JES2 resources
G    Compare users   Compare access and/or connect
```

Figure 128. RACF Reports menu

These reports come in different categories:

- Reports that combine data from several profiles and from profiles and resource information are available from options **RA.3.1** - **RA.3.6**, **RA.3.D**. For additional information about these reports, see `REPORT <reporttype>` in Chapter 13, "SELECT/LIST Fields," on page 953.
- Special function panels are available from options **RA.3.7** through **RA.3.9**, and **RA.3.G**.
- Class-specific profile query panels are available from options **RA.3.A** through **RA.3.C**.
- Application-specific overview panels are available from options **RA.3.E** and **RA.3.F**.

Note: Reports of special interest for status auditing are available from option **AU.S**. These reports include special reports on the protection of sensitive data sets, APF-authorized programs, Program Access to Data Sets (PADS) and STCs. For more information, see "STATUS AUDIT - RACF resource" on page 316 and the overviews of the GLOBAL and STARTED classes described in "STATUS AUDIT - RACF control" on page 266.

The line commands available from the **RA.R** menu option panels depend on the `ENTITY` type (user, group, data set, or general resource profile). The commands listed on a panel are the same line commands listed for the standard displays for these entity types, except for reports that show combined data from multiple profiles or from profiles and resources. On these reports, either the default line command set as explained in Table 18 on page 54 applies, or the specific options are explained separately.

Table 121 provides an overview of the RACF Report menu options with references to more detailed information.

Table 121. RA.R Report menu options

Menu option	Purpose
"RA.3.1 Profiles - Profiles with their data sets" on page 196	Reports on selected profiles in the DATASET and general resource classes, along with their access list, UACC, and auditing requirements.

Table 121. RA.R Report menu options (continued)

Menu option	Purpose
"RA.3.2 Non redundant - Data set profiles different from less specific profiles" on page 201	Understand what data sets are protected and how they are protected. The report filters out profiles that are considered redundant because they provide the same access as the next most specific profile, and then reports on the data sets for the most specific remaining profiles.
"RA.3.3 Redundant - Finding and removing redundant profiles" on page 205	Report on redundant profiles that are candidates for removal because they provide the same access as another more specific profile.
"RA.3.4 Permit/Scope - Report access of a user or group" on page 207	Overview of all resources a user or group has access to. The access can be explicit access through a `CONNECT` or `PERMIT`, or implicit access through the UACC.
"RA.3.5 OUT OF GROUP - Group data sets that can be accessed from outside the group" on page 212	Provides information about group data sets that have the potential to be accessed by users or groups outside of the group.
"RA.3.6 Non default - Reporting nonstandard data set access lists" on page 214	Overview of profiles that have access control that does not comply to the default access control specified in security policy.
"RA.3.7 MATCH - Find profiles that cover a data set or resource" on page 216	Identify all profiles that can cover a specified data set or resource name. RACF uses the most specific profile to protect a resource or data set. However, you can use this display to see what *other* profiles might also protect the resource.
"RA.3.8 GROUP TREE - Group tree display" on page 217	View all group profiles in a format indicating the group-tree structure. You can use selection criteria to specify parts of the group tree to select or exclude.
"RA.3.9 USERDATA - User data management" on page 219	Find and view installation-defined User fields and change the `userdata`.
"RA.3.A TAPEVOL - Tape Profile Overview" on page 222	Shows information about `TAPEVOL` profiles that fit the selection criteria. This report is a variant of the General Resource Profiles panel geared towards the `TAPEVOL` class.
"RA.3.B RACFVARS - RACF variable profiles" on page 225.	Shows information about RACF variables profiles that fit the selection criteria that you specify.
"RA.3.C APPL - Application profiles" on page 227	Shows a list of all RACF profiles in the `APPL` class. These profiles control the access permissions to some applications like IMS™ or CICS. On the resulting display panel, you can use action characters to work with the profiles.
"RA.3.D JES/328X - Jes/328X definitions and log data sets" on page 228	Work with JES/328X related dataset profiles and, optionally, list the data sets they cover such as the JES/328X log data sets.
"RA.3.E SDSF - SDSF command and display authorities" on page 228	See an overview of all profiles that affect SDSF security. Line commands are available to work with the profiles.
"RA.3.F JES2 - Access to JES2 resources" on page 229	See an overview of all profiles that affect JES2 security. Line commands are available to work with the profiles.

Table 121. RA.R Report menu options (continued)

Menu option	Purpose
"RA.3.G Compare users - Compare access and/or connect" on page 230	Compare user ID access in two different ways: Through permits with an option to include group permits, or compare connects for up to four user IDs.

RA.3.1 Profiles - Profiles with their data sets

The **RA.3.1 Profiles** menu option shows selected profiles in the DATASET and general resource classes, along with their access list, UACC, and auditing requirements. In this report, you can request the names of data sets covered by the profile to be added. In contrast to the LD DSNS parameter in RACF, this report also includes uncataloged data sets on disk, uncataloged migrated data sets, tape data sets from a tape management catalog, the original data set names for backed-up discrete profiles, and single-qualifier data set names. Because of the cross referencing capability this REPORT PROFILES offers a different approach from a standard profile view in RACF. However, some line commands available on the standard RACF profile view are not supported from this zSecure profile view.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                         zSecure Suite - RACF - Reports Profiles
Command ===>

Show profiles that fit all of the following criteria:
Class name  . . . . ________     (class or filter)
Profile pattern . . SYS*.**_____________________________________ (EGN mask)
High level qual . . ________     (qualifier or filter)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to select option(s)
/  Show data sets covered by each profile
   _  Including data sets on scratch tapes
_Show general resources covered by each profile

_  Output in print format
   _  Start each user or group on a new page
```

Figure 129. Report profiles selection panel

The following selection criteria are supported.

Table 122. Profile Report - available selection criteria

Selection criteria	Description
Class name	Limit to this class, or classes matching this filter
Profile pattern	Limit to profiles matching this pattern.
High level qual	Limit to profiles with this HLQ as modified by `ICHCNX00` (if present), or an HLQ matching this filter
Complex	In a complex with this name, or a matching complex if a filter is used.

The following options customize the output.

Table 123. Profile report - options for customizing output

Option	Description
Show data sets covered by each profile	Include the data set names covered with each profile
Including data sets on scratch tapes	Include even those data sets that can be overwritten at any time because the tapes they are on are in scratch status. This option is only meaningful if you asked for inclusion of data sets in the first place.
Show general resources covered by each profile	Include sensitive resources and a supported subset of other general resources covered by the resource profile (zSecure Audit only)
Output in print format	Generate output in a printable format instead of in an ISPF table
Start each user or group on a new page	Issue a form feed whenever a new HLQ is started. This option is only meaningful if you are generating output in print format.

A sample class selection display is shown in the following figure.

```
zSecure Suite PROFILE OVERVIEW                              Line 1 of 6
Command ===>                                                 Scroll===> CSR
                                                    10 Feb 2011 00:05
   Complex  Profiles MaxUacc
   TODAY         107 UPDATE
   Class    Profiles MaxUacc
__ APPCPORT         1 NONE
__ APPL             1 NONE
s_ DATASET         99 UPDATE
__ JESINPUT         2 READ
__ SECLABEL         3 NONE
__ VTAMAPPL         1 NONE
****************************** BOTTOM OF DATA ********************************
```

Figure 130. Report profile overview

The following fields of interest are shown.

Table 124. Profile report class selection - fields of interest

Field	Description
Complex	The complex name (which database)
Profiles	The number of profiles selected
MaxUacc	The highest universal access found for any selected profile
Class	The profile class
Profiles	The number of profiles selected within the class
MaxUacc	The highest universal access found for any profiles selected within the class

A profile level display is shown in the following figure.

```
zSecure Suite PROFILE OVERVIEW                                  Line 1 of 135
Command ===> _____________________________________________ Scroll===> CSR
                                                 3 Mar 2001 00:07
   Complex  Profiles MaxUacc
   TODAY         143 UPDATE
   Class    Profiles MaxUacc
   DATASET       135 UPDATE
   Profile name                                  Volume UACC    S/F Erase
__ SYSAPPL.**                                           NONE___ __R NO___
__ SYSAPPL.CNRACF.**                                    NONE___ __R NO___
__ SYSAPPL.CNRACF.BACK1DAY.**                           NONE___ __R NO___
__ SYSAPPL.GTF.**                                       NONE___ __R NO___
__ SYSAPPL.OS%%%ETP.**                                  NONE___ __R NO___
__ SYSMVIEW.*.**                                        NONE___ __R NO___
__ SYSMVIEW.V1R1M0.SEFMLINK                             NONE___ U_R NO___
__ SYSP.*.**                                            NONE___ __R NO___
__ SYSP.**.HFS                                          NONE___ U_R NO___
S_ SYSP.CPAC.T.**                                       NONE___ __R NO___
__ SYSP.CPAC.T.LOADLIB                                  NONE___ U_R NO___
__ SYSP.C##.P1.*.**                                     NONE___ __R NO___
__ SYSP.C##.P1.SYSLOG.**                                NONE___ __R NO___
__ SYSP.DINO*.**                                        NONE___ R_R YES__
```

Figure 131. Report profile level overview

The following fields of interest are shown.

Table 125. Profile Report - profile level class selection fields of interest

Field	Description
Profile name	The profile name
Volume	Volume the profile applies to (if specific)
UACC	The universal access level
Success	Effective success audit level
Failure	Effective failure audit level
Erase	Erase-on-scratch setting

The line commands available here are **L** List, **D** Delete, **C** Copy and **S** Select. The latter brings up a detail display as shown in the following figure.

```
zSecure Suite PROFILE OVERVIEW                                  Line 1 of 35
Command ===> ____________________________________________ Scroll===> CSR
                                          3 Mar 2001 00:07
   Complex  Profiles MaxUacc
   TODAY         143 UPDATE
   Class    Profiles MaxUacc
   DATASET       135 UPDATE
   Profile name                                Volume UACC    S/F Erase
   SYSP.CPAC.T.**                                     NONE      R NO
  Type    Profile name                                Volume
  GENERIC SYSP.CPAC.T.**
   nvsam  SYSP.CPAC.T.DOCLIB                          SYSP00
   nvsam  SYSP.CPAC.T.SCPPCENU                        MIGRAT
   clustr SYSP.CPAC.T.SCPPEENU                        SYSP01
    migcl SYSP.CPAC.T.SCPPEENU                        MIGRAT
   clustr SYSP.CPAC.T.SCPPHENU                        SYSP01
    migcl SYSP.CPAC.T.SCPPHENU                        MIGRAT
   nvsam  SYSP.CPAC.T.SCPPLOAD                        MIGRAT
   nvsam  SYSP.CPAC.T.SCPPMENU                        MIGRAT
   nvsam  SYSP.CPAC.T.SCPPPENU                        MIGRAT
   nvsam  SYSP.CPAC.T.SCPPSENU                        SYSP00
   nvsam  SYSP.CPAC.T.SCPPTENU                        MIGRAT
   clustr SYSP.CPAC.T.SCPPVENU                        SYSP01
    migcl SYSP.CPAC.T.SCPPVENU                        MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.LOADLIB                MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.LOG                    MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPAENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPBENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPCENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPEENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPHENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPLOAD               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPMENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPOENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPPENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPSENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPTENU               MIGRAT
   nvsam  SYSP.CPAC.T.ST010232.SCPPUENU               MIGRAT
   nvsam  SYSP.CPAC.T.VB.SCPPCENU                     MIGRAT
  Full profile name
  SYSP.CPAC.T.**
  Id       Access  Via                    Name                Data
_ SYSAUTH  OWNER                                              AUTHORIZATION G
_ C##BER2  ALTER                          ERIC TWAIN
_ STRTASK  UPDATE                         DIV STARTED TASK USR
_ SYSPROG  ALTER                                              SYSTEM PROGRAMM
```

Figure 132. Report profile detail display

The following fields of interest are shown.

Table 126. Profile Report - detail display fields of interest

Field	Description
Type	Shows the profile type for profiles (the first line). For other resources, shows the type of data set or resource. For the resources (the other lines), the type of data set or resource. Available types are listed in Table 127 on page 200.
Profile name	The profile name, followed by the names of the data sets or resources covered (if requested).
Volume	The volume the profile applies to/the data set resides on.
Full profile name	The full profile name up to 246 characters.
Id	Userid or group ID that has access on this profile.
Access	The access level.

Table 126. Profile Report - detail display fields of interest (continued)

Field	Description
Via	Condition under which access applied (for a conditional entry): class and profile name, or blank.
Name	For a user ID in the Id column the user name is shown here.
Data	Installation data for the user or group.

The data set types that can be shown are listed in the following table.

Table 127. Profile Report - Data set types

Data set type	Description
nvsam	Non-VSAM disk data set, migrated if the volume status is `MIGRAT` for `HSM` or `ABR`, or archived if the volume is ARCIVE for `DMS`. This information is obtained from the VTOC for data sets on disk, the HSM MCDS and the `ABR` ACF for migrated data sets, and the `DMSFILES` data set for archived data sets. The information is not derived from the catalog entries.
clustr	VSAM cluster (catalog entry). The volume listed is the volume of the catalog. The source for the cluster names can be one of the following: a catalog, an `HSM MCDS`, `ABR ACF`, `DMS DMSFILES` data set, or `VVDS`.
bkpclu	Backup of a VSAM cluster. Normally, this is only listed below a backed-up discrete profile (for example, a discrete profile with a system-generated name). The source for the cluster name is either the `HSM BCDS` or a `DMS DMSFILES` data set.
index	Index component of a VSAM cluster residing on the indicated DASD volume.
data	Data component of a VSAM cluster residing on the indicated DASD volume.
aixix	Index component of a VSAM alternate index residing on the indicated DASD volume.
aixda	Data component of a VSAM alternate index residing on the indicated DASD volume.
migcl	Migrated or archived VSAM cluster. This is listed below a cluster entry instead of the components. The volume is equal to MIGRAT or ARCIVE.
clust	Backup of VSAM cluster. This is listed below a bkpclu entry instead of the components. The volume is equal to MIGRAT or ARCIVE.
gag	Base name of a GDG (Generation Data Group), obtained from a catalog.
cnntap	Cataloged, non-managed tape file, on a non-managed volume.
unntap	Uncataloged, non-managed tape file, on a non-managed volume. The source for such an entry is probably the `TVTOC` of a `TAPEVOL` profile.
cmmtap	Cataloged, managed tape file on a managed, nonscratch tape volume.
ummtap	Uncataloged, managed tape file on a managed, nonscratch tape volume.
cnmtap	Cataloged, non-managed file on a managed, non-scratch volume. This means that the catalog entry conflicts with the tape management information.
unmtap	Uncataloged, non-managed file on a managed, non-scratch volume. The source for such an entry is probably the `TVTOC` of a `TAPEVOL` profile.
cnstap	Cataloged, non-managed file, on a managed volume in scratch status.
unstap	Uncataloged, non-managed file, on a managed volume in scratch status. The source for such an entry is probably the TVTOC of a `TAPEVOL` profile.

Table 127. Profile Report - Data set types (continued)

Data set type	Description
secvol	Secondary volume of a multi-volume data set.
sensr-r	General resource (not a data set) that is sensitive if read access is permitted.
sens-w	General resource profile that is sensitive if update access is permitted.
sens-a	General resource (not a data set) that is sensitive if alter access is permitted.
priv	General resource (not a data set) that gives the user some privilege.

In print format, the report looks like the report shown in the following figure.

```
 BROWSE - C##BJT2.C2R1EF2A.REPORT ------------------------------------------------------------------------- LINE 00000000 COL 001 132
 COMMAND ===>                                                                                                SCROLL ===> CSR
********************************************************* Top of Data ********************************************************************
zSecure Admin PROFILE OVERVIEW complex TODAY    class APPCPORT  3 Nov 2011 00:07                                      page    1

Type    Profile name                                Volume Id       Access  When                  UACC    Success Failure Erase
        SYSPLU01                                           C##BMR1  OWNER                         NONE            READ    NO
                                                           STRTASK  READ
zSecure Admin PROFILE OVERVIEW complex TODAY    class APPL      3 Nov 2011 00:07                                      page    2

Type    Profile name                                Volume Id       Access  When                  UACC    Success Failure Erase
        SYSPLU01                                           C##BMR1  OWNER                         NONE            READ    NO
                                                           STRTASK  READ
zSecure Admin PROFILE OVERVIEW complex TODAY    class DATASET   3 Nov 2011 00:07                                      page    3

Type    Profile name                                Volume Id       Access  When                  UACC    Success Failure Erase
GENERIC SYSAPPL.**                                         SYSPROG  OWNER                         NONE            READ    NO
 nvsam  SYSAPPL.CNRACF1.UNLOAD                     TSTUS1 C##BSUPP READ
 nvsam  SYSAPPL.C2R32AE.UNLOAD                     TSTUS1 C##A     READ
 nvsam  SYSAPPL.CNRACF4.UNLOAD                     TSTUS1 SYSAPPL  ALTER
 nvsam  SYSAPPL.EPR.SMFDUMPW.G0153V00              EPRPAG SYSPROG  ALTER
 nvsam  SYSAPPL.EPR.SMFDUMPW.G0154V00              EPRPAG
 nvsam  SYSAPPL.EPR.SMFDUMPW.G0155V00              EPRPAG
 nvsam  SYSAPPL.EPR.SMFDUMPW.G0156V00              EPRPAG
 nvsam  SYSAPPL.EPR.SMFDUMPW.G0157V00              EPRPAG
 gdg    SYSAPPL.SMFDUMPW
```

Figure 133. Report profile print format

Notes:

1. Listing the data sets covered requires a CKFREEZE file, and furthermore that *VSAM data sets are not listed if no catalog dump was included.*
2. For advanced users: if you want to write your own REPORT_PROFILES query, the data sets covered can be included by means of the REPORT DATASETS command; to include data sets on scratch tapes as well, also add the SCRATCH keyword.

RA.3.2 Non redundant - Data set profiles different from less specific profiles

The **RA.3.2 Non redundant** menu option is designed to help you understand what data sets are protected and how they are protected. The report filters out profiles that are considered redundant because they provide the same access as the next most specific profile. The report includes he data sets for the most specific remaining profiles. The criteria for determining whether profiles are redundant are explained in "RA.3.3 Redundant - Finding and removing redundant profiles" on page 205.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - RACF - Reports Non redundant
Command ===>

Show profiles that fit all of the following criteria:
Profile pattern . . _____________________________________________________ (EGN mask)
High level qual . . C##BJTI_     (qualifier or EGN mask; reduces time)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to select option(s)
/  Show datasets covered by each profile
   _  Including datasets on scratch tapes

_  Output in print format
   _  Start each user or group on a new page
```

Figure 134. Report Non redundant selection panel

The following selection criteria are supported.

Table 128. Non-Redundant Profile Report - selection criteria

Selection Criteria	Description
Profile pattern	Limit to profiles matching this pattern.
High level qual	Limit to profiles with this HLQ as modified by ICHCNX00 (if present), or an HLQ matching this filter
Complex	In a complex with this name, or a matching complex if a filter is used.

The following options customize the output.

Table 129. Non-Redundant Profile Report - custom output options

Option	Description
Show data sets covered by each profile	Include the data set names covered with each profile
Including data sets on scratch tapes	Include even those data sets that can be overwritten at any time because the tapes they are on are in scratch status. This option is only meaningful if you asked for inclusion of data sets in the first place.
Output in print format	Generate output in a printable format instead of in an ISPF table
Start each user or group on a new page	Issue a form feed whenever a new HLQ is started. This option is only meaningful if you are generating output in print format.

A sample display is shown in Figure 135.

```
Non-redundant dataset profiles                                  Line 1 of 1
Command ===>                                                  Scroll===> CSR
                                          10 Feb 2011 14:56
   Complex  Timestamp         Profiles
   DEFAULT  10 Feb 2011 14:56        1
   Qual     Profiles
   C##BJTI         1
   Type    Volume Profile name                                First reason
s_ GENERIC        C##BJTI.**                                  No generic
****************************** BOTTOM OF DATA ********************************
```

Figure 135. Report NONREDUNDANT profile level display

In this example, the only profile in the query results for the HLQ specified of interest is C##BJTI.**, which is non-redundant because a more generic profile does not exist to take over its role.

The following fields of interest are shown.

Table 130. Non-redundant Profile Report - field descriptions

Field	Description
Complex	The name of the complex
Timestamp	The date and time to which the information pertains
Profiles	The total number of profiles selected
Qual	The first qualifier of this set of profiles (after ICHCNX00 processing)
Profiles	The number of profiles selected with that HLQ
Type	The profile type
Volume	The volume the profile pertains to (if volume-specific)
Profile name	The profile name
First reason	Indicates why this profile is selected. See Table 131.
UACC	The Universal Access of the profile
S/F	The effective success and failure audit levels (separated by a blank).
Era	The Erase-on-scratch settings of the profile

Table 131 lists the reasons that a profile can be considered non-redundant.

Table 131. Non-redundant Profile Report - reasons for profile selection

Reason for selection	Description
- candidate -	This is a generic profile or entry in the global access table that was the most specific matching generic for one of the profiles considered non-redundant.
- redundant -	This field is only present if you requested REPORT REDUNDANT. It marks all profiles that were considered redundant.
Access	The access level of a user or group in the access list of this profile was different from the access level in the access list of the candidate profile for the same identity (user or group), and it was not overruled anyway by an entry in the global access table. The entry is one of the entries marked with an arrow.
Audit	The audit requirements are different from the candidate generic profile.
Erase	The erase-on-scratch requirement is different from that of the candidate generic profile. These profile requirements are not considered if the ERASE(ALL) or NOERASE global options are active.
Extra group	The access list of this profile contains a group that is not present on the access list of the candidate generic profile. It is one of the entries marked with an arrow.
Missing group	The access list of this profile does not contain a group that is present in the access list of the candidate generic profile. You must look up the candidate profile access list to see which group. No arrow is present.

Table 131. Non-redundant Profile Report - reasons for profile selection (continued)

Reason for selection	Description
Missing user	The access list of this profile does not contain a user ID that is present in the access list of the candidate generic profile. That user ID is also not given the same access through a Connect. You must review the candidate profile access list to see which group has the missing user ID. No arrow is present.
No generic	There is no matching generic to serve as candidate.
Undefined id	There is an extra user or group present in the access list that is not present in the access list of the candidate generic profile. However, the user or group was not defined.
Used as model	The profile is used as a model on a USER or GROUP profile and hence not redundant.
User no connect	Might also be called Extra User. A user ID is present in the access list that is not present in the access list of the candidate profile. Nor does that user have a connection to any of the groups present in the access list of the candidate generic profile. The user ID is indicated by an entry marked with an arrow.
User privileged	A user ID is present in the access list that is given more access than the equivalent entry in the access list of the candidate profile, which is either the user ID or the connect group giving the highest access. The user ID is indicated by an entry marked with an arrow. You have to look at the candidate profile access list to find the access level involved.
User restricted	A user ID is present in the access list that is given less access than the equivalent entry in the access list of the candidate profile, either the user ID or the connect group giving the highest access. The user ID is indicated by one of the entries marked with an arrow. You must review the candidate profile access list to find the access level involved.
Universal access	UACC is different from the candidate profile UACC.

A detail display is shown in Figure 136.

```
Non-redundant dataset profiles                                  Line 115 of 130
Command ===>                                                    Scroll===> CSR
                                                  10 Feb 2011 14:56
  Type    Volume Profile name                                  First reason
    migcl MIGRAT C##BJTI.TESTARES.VSAM.CLUSTER3
   clustr SYS102 C##BJTI.TESTARES.VSAM.CLUSTER5
    migcl MIGRAT C##BJTI.TESTARES.VSAM.CLUSTER5
   nvsam  MIGRAT C##BJTI.TESTIN
   nvsam  MIGRAT C##BJTI.TESTIN2
   nvsam  MIGRAT C##BJTI.TESTTLMS.CKFREEZE
   nvsam  MIGRAT C##BJTI.UTOOLS.ESDTLS
   nvsam  SM3005 C##BJTI.WR809058.CKFREEZE
  Complex  UACC    S/F Erase Owner
  DEFAULT  NONE___ __R NO_   C##BJTI_
  Dif Id      Access  Via      Name                Data
     C##BJTI  OWNER            JOYCE TIMBER
     C##BJTI  QUALOWN          JOYCE TIMBER
     C##AINT  ALTER            Zsecur GROUP ADMIN
     C##BJT2  ALTER            JOYCE TIMBER
     C##B     READ                                 PERSONNEL
****************************** BOTTOM OF DATA ********************************
```

Figure 136. Report NONREDUNDANT detail display

The following fields of interest are shown.

Table 132. Non-redundant Profile Report - detail display fields

Field	Description
Type	For the profile (the first line), the profile type. For the data sets (the other lines), the type of data set; see the table in "RA.3.1 Profiles - Profiles with their data sets" on page 196.
Volume	The volume the profile applies to/the data set resides on.
Profile name	The profile name, followed by the names of the data sets covered (if requested).
Complex	The complex name
UACC	The universal access level
S/F	The effective success and failure audit levels (separated by a blank).
Erase	Erase-on-scratch setting
Owner	The profile owner
Dif	Indicates whether this access list entry makes a difference. This column contains an arrow if the access ID is listed for another reason other than being redundant.
Id	Userid or group ID that has access on this profile
Access	The access level
Via	Condition under which access applied (for a conditional entry), or blank
Name	For a user ID in the Id column the user name is shown here
Data	Installation data for the user or group

Figure 137 provides an example of the output in print format.

```
N O N - R E D U N D A N T   D A T A S E T   P R O F I L E S   complex DEFAULT  qualifier C##BJTI  10 Feb 2011 00:05

Type    Volume Profile name                                  Id       access  program  UACC    Success Failure Era First reason
GENERIC        C##BJTI.**                                    C##BJTI  OWNER            NONE            READ        No generic
 nvsam  MIGRAT C##BJTI.ASMIDF.CMDLOG                         C##BJTI  QUALOWN
 nvsam  MIGRAT C##BJTI.AUDION.CNTL                           C##AINT  ALTER
 nvsam  SM3003 C##BJTI.CERT                                  C##BJT2  ALTER
 nvsam  ETPSMS C##BJTI.CNFCOLL.TRS                           C##B     READ
 nvsam  ETPSMS C##BJTI.CNFCOLL.XM
 nvsam  SM3001 C##BJTI.CNFTEST.CKFREEZE
```

Figure 137. Report NONREDUNDANT print format

RA.3.3 Redundant - Finding and removing redundant profiles

Use the **RA.3.3 Redundant** menu option for reporting on the access list of dataset profiles to identify redundant profiles that can be removed. The report includes data set profiles in the following categories:

- Profiles not covered by a less specific generic profile.
- Profiles covered by a less specific generic profile where the `WARNING` `AUDIT`, or `ERASE` (if active globally) settings are different.
- Profiles where the access list is different so they cannot be considered similar.

  Access is considered similar if the access list contains the group to which the dataset belongs with a lower level than present in GLOBAL DATASET member `&RACGPID.*` (no EGN), `&RACGPID.**` or `&RACGPID.*.**` (EGN). Access is also considered similar if a user ID is present on the discrete profile access list with an access that is also granted through one of the groups to which the user ID is connected.

Redundant profiles are identified with a `- redundant -`.

A sample display is shown in Figure 138. For additional information about the report and how to interpret it, press F1 on the panel for help.

```
Redundancy analysis of dataset profiles                          Line 1 of 3
Command ===>                                                    Scroll===> CSR
                                                  10 Feb 2011 15 55
   Complex  Timestamp         Profiles Non-redundant
   DEFAULT  10 Feb 2011 15:55        3             1
   Qual     Profiles Non-redundant
   C##BJTI         3             1
   Type    Volume Profile name                                  First reason
__ GENERIC        C##BJTI.**                                    - candidate -
__ GENERIC        C##BJTI.**                                    No generic
__ GENERIC        C##BJTI.RE.DUN.DANT.**                        - redundant -
****************************** BOTTOM OF DATA ********************************
```

Figure 138. Report REDUNDANT profile level display

This panel shows two separate profiles, but counts three. The middle entry C##BJTI.**, which is the same as the one shown in Figure 134 on page 202, is not redundant because it is a top-level profile (*No generic*). The last entry shows the other, redundant, profile C##BJTI.RE.DUN.DANT.**. The first entry shows that C##BJTI.** is a -candidate- profile, which means that this profile might take over the role from one or more profiles flagged redundant if they were removed.

If the administration product zSecure Admin is installed and not disabled (that is, not only zSecure Audit for ACF2), then the selection panel for this option provides an extra output option *Remove redundant profiles* that means no report is to be generated at all, but instead the REMOVE REDUNDANT function is to be performed. This function generates the RACF commands to remove all profiles marked as redundant in the analysis.

This REMOVE REDUNDANT function is designed specifically to aid in the conversion from ADSP to generic profiles. When you use this function, it automatically generates commands to delete discrete profiles that provide *equivalent* access to the access provided by the combination of the most specific matching generic data set profile and the most specific matching global access table entry (if present).

If you use Automatic Backup and Recovery (ABR) with the PROFKEEP option, be aware that on restore of a non-VSAM data set that must be recreated, the ABR function requests a default discrete profile to be created through ADSP if its RACF indicated bit was set on migration. In addition, this RACF indicated bit is only available on the migration tapes which currently are not checked. Instead, it is assumed that an existing discrete profile applies. If a data set is already allocated, ABR prevents the restore unless the RACF indicated bits match. Therefore, if you are converting from ADSP to generic profiles, consider the implications regarding ABR and take them into consideration when you are reviewing the remove profile commands generated by the REMOVE REDUNDANT function.

For a profile to be considered *redundant*, three profile properties are checked:

1. Access requirements (access list, conditional access list, and universal access).
2. Audit requirements (failure audit level, success audit level).
3. Erase-on-scratch requirement.

The first two items are simply compared to those of the most specific matching generic profile, called the *candidate* profile. They must be equal before the profile is considered redundant. However, the *erase-on-scratch* requirement is not checked if the system wide option ERASE(ALL) or NOERASE is active.

The access requirement comparison is more complicated. Simplest is the *universal access* (UACC) comparison. For a profile to be considered redundant, its UACC must either be equal to that of the candidate profile, or less than ALTER and at the same time less than or equal to the most specific matching entry of the Global Access Table (that is, a member of the DATASET profile in class GLOBAL).

The *access list* and *conditional access list* comparison takes into account group membership of user IDs in the list. That is, a user ID in the conditional list of a redundant profile might be missing from the conditional access list of the candidate profile only, if one of the connect groups is present with the same access (and the same program name), and no connect groups are present with a higher access (and the same program name).

The redundancy check does not take all fields into account. For example, the RESOWNER and NOTIFY fields, security categories, levels, and labels are not checked.

For advanced users who want to provide extra selection criteria in the preamble or specify a modified query of type REPORT_REDUNDANCY or REMOVE REDUNDANT: Do not exclude profiles from the USER, GROUP, or GLOBAL classes. These classes might be needed for determining whether profiles are redundant. For example, when excluding a certain HLQ, specify EXCLUDE QUAL=*id* CLASS=DATASET!

RA.3.4 Permit/Scope - Report access of a user or group

The **RA.3.4 PERMIT/SCOPE** menu option provides an overview of all resources a user or group has access to. The access can be explicit access granted through a connect or permit, or implicit access granted through the UACC.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                         zSecure Suite - RACF - User Scope/permit
Command ===>

Id  . . . . . . . . C##BJTI_ C##BJT2_ ________ ________ ________ ________

Specify type of authorization
  1  1. Direct permit to the Id (Id on access list)
     2. Direct permit or Connect (Id or Connect Group on access list)
     3. Scope (access or administrative authority by any means)

Report options
 Minimum access to show              Specify output options
 8  1. Execute     2. Read           _  Show resources covered by profile
    3. Update      4. Control           _  Including datasets on scratch tapes
    5. Alter       6. Admin          _  Output in print format
    7. Owner       8. Show all          _  Start each Id on a new page

Select profiles to include. Blank profile field(s) to include missing profiles
 Dataset HLQ . . . . *_______  (qualifier or filter, * for all, blank for none)
 Dataset profile . . ____________________________________________ (EGN mask)

 Other class . . . . *_______  (class or filter, * for all, blank for none)
 Other profile . . . ____________________________________________ (EGN mask)
```

Figure 139. Report Scope/Permit selection panel

The following selection criteria and output options are available.

Table 133. User Scope/Permit Report - selection criteria and custom output options

Selection Criteria or Output Option	Description
Id	Up to six user or group IDs for which you want this function performed
Specify type of authorization	Specify the access type you want to include in the report or display: **1** for a PERMIT to the Id, **2** for access via PERMIT or CONNECT, or **3** for access by any means.
Minimum access to show	The minimum access level for inclusion in the report
Show resources covered by each profile	Include the resource names covered by each profile.
Including data sets on scratch tapes	Include even those data sets that can be overwritten at any time because the tapes they are on are in scratch status. This option is only meaningful if you asked for inclusion of data sets in the first place.
Output in print format	Generate output in a printable format instead of in an ISPF table
Start each Id on a new page	Start each separate report on a new page. This option is only meaningful if you are generating output in print format.
Dataset HLQ	Limit the DATASET class to profiles with this HLQ as modified by `ICHCNX00` (if present), or an HLQ matching this filter.
Dataset profile	The `EGN` mask that a profile in the DATASET class must match to be included in the report.
Other class	Mask for the selection of General Resource classes
Other profile	The `EGN` mask that a profile in a General Resource class must match to be included in the report.

Figure 140 provides a sample of the Report Permit Overview panel.

```
zSecure Admin REPORT PERMIT - Explicit access     1 s elapsed, 0.3 s CPU
Command ===>                                                 Scroll===> CSR
                                                 10 Feb 2011 17 00
   Complex  Scope of Profiles HighAcc
s_ DEFAULT  C##BJTI        48 ALTER
__ DEFAULT  C##BJT2        33 ALTER
****************************** BOTTOM OF DATA ********************************
```

Figure 140. Report Permit overview

The following fields of interest are shown.

Table 134. User Scope Permit Report - explicit access fields

Field	Description
Complex	The complex name.
Scope of	The IDs the report was requested for.
Profiles	The number of profiles found for this id.
HighAcc	The highest access the id has on any of the profiles.

This selection level is skipped if you requested the report for only one ID.

Figure 141 shows a sample of the Report Permit Class Selection panel.

```
zSecure Admin REPORT PERMIT - Explicit access                Line 1 of 2
Command ===>                                                  Scroll===> CSR
                                                  10 Feb 2011 17:00
   Complex  Scope of Profiles HighAcc
   DEFAULT  C##BJTI        48 ALTER
   Class    Profiles HighAcc
s_ DATASET        45 ALTER
__ FACILITY        3 READ
****************************** BOTTOM OF DATA ********************************
```

Figure 141. Report Permit class selection display

On this level the classes are listed with the number of profiles selected in them and the highest access of the ID on any of those profiles.

```
zSecure Admin REPORT PERMIT - Explicit access              Line 1 of 11
Command ===>                                                 Scroll===> CSR
                                                  10 Feb 2011 17:00
   Complex  Scope of Profiles HighAcc
   DEFAULT  C##BJTI        16 ALTER
   Class    Profiles HighAcc
   DATASET        13 ALTER
   Class    Profile name                                 Access  Via
__ DATASET  C##A.D.CNFJTI.**                             ALTER   C##BJTI
__ DATASET  C##A.D.CNRJTI.**                             ALTER   C##BJTI
__ DATASET  C##A.D.CNRNEW.SC2RSAMP                       UPDATE  C##BJTI
__ DATASET  C##A.D.CNRNEW*.**                            UPDATE  C##BJTI
__ DATASET  C##A.D.HLLJTI.**                             ALTER   C##BJTI
__ DATASET  C##A.L.**                                    READ    C##BJTI
__ DATASET  C##A.P.SMPMCS.CNTL                           READ    C##BJTI
__ DATASET  C##BJT2.**                                   ALTER   C##BJTI
__ DATASET  C##BMCO.**                                   READ    C##BJTI
s_ DATASET  SYSAPPL.CNRACF.**                            READ    C##BJTI
__ DATASET  SYSAPPL.CNRACF.BACK1DAY.**                   READ    C##BJTI
****************************** BOTTOM OF DATA ********************************
```

Figure 142. Report Permit profile display

The following information is provided on the profile level of the report.

- List of profiles
- Access level
- Access list id through which this access is granted. For conditional access, the information also reports when the access is granted

If the data sets covered by each profile are to be shown, they are listed on the detail display.

The only line commands available on this panel are **S** Select and **D** Delete.

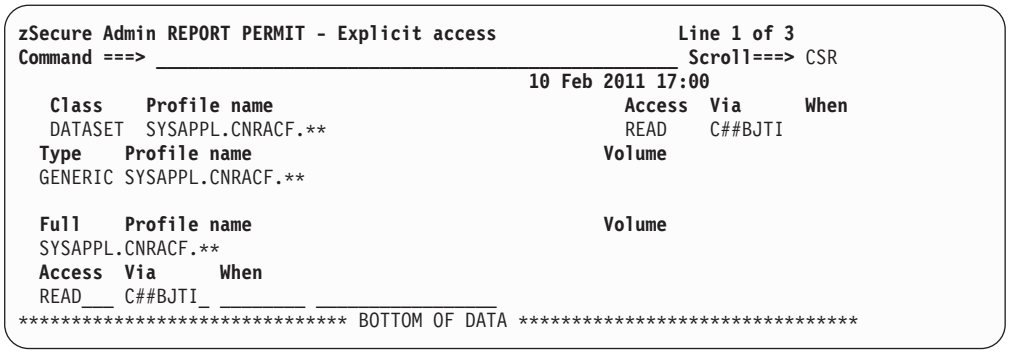


Figure 143. Report Permit detail display

The detail display shows the same information available on the record level display. However, you can also see the full profile name, up to 246 characters and modify the access allowed value.

The philosophy of the REPORT SCOPE function is to show the profiles, and optionally the resources to which the user or group *directly* or *indirectly* has access. Indirect access is the ability to modify a profile to give oneself direct access. The report includes access through the following group attributes: SPECIAL, OPERATIONS, and AUDITOR. To prevent inadvertent listing of all or almost all profiles in the system, access through the system-wide special, operations, and auditor attributes are *not* included. The report does include information about the following access types:

- Access through universal access and warning mode of profiles.
- Access through the global access table.
- Access through missing profiles.
- Access through discrete/generic DATASET profiles mismatches (in a NOPROTECTALL environment).

Because the SCOPE function includes so many different access types, it tends to produce a large quantity of output. To generate more manageable output, use the selection criteria described in Table 133 on page 208. In addition to the selection criteria, the SCOPE function also provides the follow-up panel shown in Figure 144 on page 211 with options to exclude information for selected access methods.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                         zSecure Suite - RACF - User Permit
Command ===>

Id  . . . . . . . . C##BJTI  C##BJT2

Enter "/" to exclude access granted because of
_  Universal Access
_  Access to all RACF defined users
_  Global Access Table
_  Profiles in Warning mode allow ALTER to resource
_  Resource is not protected
_  User is group auditor, can review any profile in scope
_  User is group operations, can access resources in scope
_  User is group special, can modify any profile in scope
_  User is owner of profile
_  User can change password or password phrase of profile owner
_  User is group special, can connect to any group in scope
_  User can change his own user profile
_  User has Devolved Authorities to RACMAP resources and digital certificates
/  User has Devolved Authorities over profile
_  CLAUTH class authorization or connect CREATE/CONNECT/JOIN authority
```

Figure 144. Report Scope suppress panel

In the example above CKGOWNR access, permitted by CKGRACF authority has been suppressed. Figure 145 provides a sample report in print format.

```
U S E R   A U T H O R I Z A T I O N   F O R   I D  C##BJTI  JOYCE TIMBER        DEFAULT  10 Feb 1999 00:05

Class    Type    Profile name                                Volume Access  Via      When
APPCTP   GENERIC **                                                READ    - UACC -
CONSOLE          SDSF                                              ALTER   - WARN -
DATASET  GLOBAL  &RACUID.*.**                                       ALTER   - UACC -
DATASET  GENERIC ANF.*.**                                          READ    - UACC -
DATASET  GENERIC ANF.SANFLOAD                                      READ    - UACC -
DATASET  GENERIC AOP.*.**                                          READ    - UACC -
DATASET  GENERIC API.*.**                                          READ    - UACC -
DATASET  GENERIC ASMA.*.**                                         READ    - UACC -
DATASET  GENERIC ASMA.V1R2M0.SASMMOD1                              READ    - UACC -
```

Figure 145. Report SCOPE print format

The **Via** column shows the user ID or group in the access list entry that gave the access indicated. The value can also be any of the following:

-AUDIT-

-GLOBAL-

-RACMAP-

-RACDCT-

-SCP.G-

-SCP.ID-

-SCP.U-

- UACC -

-UNPROT-

- WARN -

- OPER -

For more information, see the “VIA” on page 1240 field description in REPORT_SCOPE NEWLIST.

The **SCP** values indicate access through the CKGRACF authorized component of Security zSecure; through a CKG.SCP.U..., CKG.SCP.G..., and CKG.SCP.ID... profile

respectively.- *AUDIT* - and - *OPER* - stand for group auditor and group operations access, respectively. In restricted mode, - *n/a* - is shown for an id that has access via the access list.

The column **Access** can show other access authorities than the conventional NONE, READ, UPDATE, CONTROL, and ALTER. These access authorities are documented with the ACCESS parameter of the REPORT command in "REPORT" on page 875.

For advanced users

If you design your own query using the REPORT_SCOPE type, you can use the SUPPRESS REASON=list command to suppress access reasons. See also "SUPPRESS" on page 932. The following reasons can be suppressed:

- *ALTER-M* to suppress accesses that would be granted because users are permitted to modify certain fields of their own user profile ('alter myself')
- *CKGOWNR* for CKGRACF-access
- *CKGRACDCERT* for access given through *IRR.DIGTCERT.** FACILITY* profiles
- *CKGRACMAP* for access given through *IRR.RACMAP.** FACILITY* profiles
- *CREATE* to suppress administrative access granted through CREATE authority on a connect and class authorization (CLAUTH) on a user.
- *GLOBAL* for global access table
- *GRPAUDIT* for propagation and consideration of group-audit authority
- *GRPOPER* for propagation and consideration of group-operations authority
- *GRPSPEC* for propagation and consideration of group-special authority
- *ID(*)* for access through the ID * on an access list
- *NOPROFILE* for unprotected data sets
- *OWNER* for owned profiles
- *PWDCHANGE* for propagation of group-special authority
- *SELFCONNECT* for propagation of group-ownership authority
- *UACC* for universal access
- *WARN* for warning mode profiles

RA.3.5 OUT OF GROUP - Group data sets that can be accessed from outside the group

The **RA.3.5 OUT OF GROUP** menu option shows permits on group data sets to users or groups outside that group. The group is taken to be the first qualifier of the dsname, optionally changed by ICHCNX00 or ICHNCV00. The report shows a group data set profiles that have a UACC other than NONE, or an OWNER or access list entry for a user outside the group or another group.

The report can be used by sites that have a simple RACF group structure with both user and data set profiles, to get a small report of profiles with a non-standard access list, as opposed to a complete list of all profiles. This is especially useful in all-discrete environments, where most of the profiles typically have a default layout.

The same selection panel as for REPORT PROFILES is used. A sample display is shown in Figure 146 on page 213.

```
Dataset profiles with permits outside group                    Line 1 of 13
Command ===>                                                  Scroll===> CSR
                                                  10 Feb 1999 18:05
   Complex  Timestamp         Profiles
   DEFAULT  10 Feb 1999 18:05       13
   Qual     Profiles
   C##B           13
   Type    Volume Profile name                                First reason
s_ GENERIC        C##B.**                                     Other group
__ GENERIC        C##B.ILM.**                                 Other group
__ GENERIC        C##B.Q.**                                   Other group
__ GENERIC        C##B.T.**                                   Other group
__ GENERIC        C##B.T.CNROLD.**                            Other group
__ GENERIC        C##B.T.C4R300T.**                           Other group
__ GENERIC        C##B.T.HLLOLD.**                            Other group
__ GENERIC        C##B.T.KEEP#ALL.**                          Other group
__ GENERIC        C##B.T.KEEP#ALL.CNGLOAD                     Other group
__ GENERIC        C##B.T.RC*.**                               Other group
__ GENERIC        C##B.T.RC941124.VSAMCOPY.SMF                Other group
__ GENERIC        C##B.T.VSAMMVT.**                           Other group
__ GENERIC        C##B.X.**                                   Other group
****************************** BOTTOM OF DATA *******************************
```

Figure 146. Report Permits outside group overview

On this display the profiles are listed that have 'foreign permissions'.

A detail display is shown in the following figure.

```
Dataset profiles with permits outside group                    Line 1 of 9
Command ===>                                                  Scroll===> CSR
                                                  10 Feb 1999 18:09
  Type    Volume Profile name                                 First reason
  GENERIC        C##B.**                                      Other group
  Complex  UACC
  DEFAULT  NONE___
  Out Id      Access  Via      Name                Data
     C##B     OWNER                                PERSONNEL
     C##B     QUALOWN                              PERSONNEL
  -> SYSPROG  ALTER                                SYSTEM PROGRAMMING
     C##B     READ                                 PERSONNEL
  -> C##A     ALTER                                MANAGEMENT
****************************** BOTTOM OF DATA *******************************
```

Figure 147. Report Permits outside group detail display

The **First reason** column indicates the first reason why a profile was included in the report. There can be more reasons, but only one is spelled out. However, *all* access list entries referring outside the data set 1st-qualifier group are marked with an arrow. The reasons that can be present are:

Universal access	UACC is unequal to NONE, giving access outside the group.
User not in group	A user in the access list or OWNER field is not connected to the data set first qualifier group. If it is a user in the access list, the user is one of the entries marked with an arrow.
Other group	A group in the access list or OWNER field was present different from the data set first qualifier group. If the group is part of the access list, it is one of the entries marked with an arrow.

Note to advanced users: be careful with excluding profiles in classes other than DATASET in REPORT_OUTOFGROUP queries for reasons similar as outlined for REPORT_REDUNDANCY.

RA.3.6 Non default - Reporting nonstandard data set access lists

Use option **RA.3.6** to select all profiles that could cover the data set or resource name specified. RACF uses the most specific profile to protect a resource or data set. However, you can use this display to see what *other* profiles could also protect the resource. This can be useful to determine if the current profile is required

This report uses the same layout as the one described in the previous section.

A report of access granted outside the data set first qualifier group is not usable if your site distinguishes the grouping of data sets (resources, objects) and the grouping of users (subjects). RACF groups are used for both of these purposes. This distinction is called the concept of *data set groups*:

Data set groups are normal RACF groups, but without *any* connected user.

This contrasts with *user groups*:

User groups are normal RACF groups with users, but without *any* group data set profile (and hence, in a PROTECTALL environment, without any data sets).

The rest of the groups might be called *common groups*:

Common groups are normal RACF groups, containing *both* user profiles and group data set profiles.

Access to the data sets in a data set group is regulated by a generic profile. In this generic profile, the user group that currently owns the data sets is listed in the Access list with ALTER authority, as well as in the OWNER field. These settings provide users with group-authority in the user group so that they have control over the owned data set group. This authority is based on a connection to a user group and does not require any connections to the data set group. It also makes it a lot easier to transfer ownership of groups of data sets from one owner (a user group) to another owner (another user group). Only the ownership of the data set group needs to be changed, not all data set profiles for the data set group.

The NONDEFAULT report has been designed to support these kinds of data set profiles as *default* or *standard* in addition to those profiles containing only the data set first-level qualifier in the access list.

For group data sets, this lists 'out-of-group' access as discussed in the previous section, as well as 'out-of-group' access where the 1st qualifier is another group than the OWNER. However, user IDs in the access list are not checked for connects, but always marked as non-default, unless they are equal to either the OWNER or the 1st qualifier (an explicit PERMIT command must have been used to create this situation, and in this sense they are non-default).

In addition, user data set profiles are listed where other people than the owner are in the access list or in the OWNER field (or UACC not equal to NONE).

If your security standards differ from the standards implied here, you might prefer to see a different interpretation of the default settings and your comments on this aspect would be welcomed (direct those to the address shown on the back of the front page of this manual).

A sample report in print format is shown in the following figure.

```
N O N - D E F A U L T   D A T A S E T   P E R M I T S   complex DEFAULT  qualifier C##B     10 Feb 1999 00:05

Type    Volume Dataset name                              First reason          UACC       Id       access  program  Name
GENERIC        C##B.**                                   Not owner or group    NONE       C##B     OWNER
                                                                                          C##B     QUALOWN
                                                                                       -> SYSPROG  ALTER
                                                                                       -> C##B     READ
                                                                                       -> C##A     ALTER
GENERIC        C##B.ILM.**                               Group access          NONE       C##AINT  OWNER            Zsecur GROUP
                                                                                          C##B     QUALOWN
                                                                                       -> C##B     READ
                                                                                       -> C##A     ALTER
                                                                                          C##AINT  ALTER
```

Figure 148. Report Non-default dataset permits print format

The column **First reason** indicates why a profile was included in the report. The report only includes one reason. Although there might be more than one reason, only one is reported. However, *all* access list entries present that are considered non-default are marked with an arrow. The reasons that can be present are:

Reason	Description
Conditional access	An entry in the conditional access list is always considered non-default.
Group access	The first qualifier for the owning group or data set must be in the access list of a group data set profile to be considered default. In addition, the access must be either ALTER or UPDATE. ALTER is the preferred way, especially in a generic profile environment with PROTECTALL active, since data set creation is otherwise impossible. However, the RACF default set by the GRPACC attribute is UPDATE, therefore this is considered default, too. The entry is marked with an arrow unless it is missing from the access list.
Missing access	To be considered default, access must be granted either to the first qualifier identity or to the owner, either implicitly if the first qualifier is a user ID or explicitly through an access list entry.
More than 1 group	For an access list to be considered the default, it can contain only one group. That group must be either the first qualifier group or the owning group. Other groups are marked with an arrow.
Not owner or group	An identity in the access list is only considered default if it is the owner, or if it is a group *and* equal to the first qualifier. An undefined identity is never considered default. The identity is one of the entries marked with an arrow.
Owner access not ALTER	To be considered default, the identity owning the profile must have ALTER access to his data.
Owner not in group	The owner of a group data set profile is a user without connect to the group. **Note:** The notion of data set groups presupposes that ownership is a user group, not a user.
Universal access	UACC is unequal to NONE, giving access outside the group.

Reason	Description
User not owner	The data set name starts with a user ID. To be considered default, the data set profile owner must be that user ID.

RA.3.7 MATCH - Find profiles that cover a data set or resource

Use option **RA.3.7** to select all profiles that could cover the data set or resource name specified. RACF uses the most specific profile to protect a resource or data set. However, you can use this display to see what *other* profiles could also protect the resource. This can be useful to determine if the current profile is required.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Match profile
Command ===> ____________________________________________________________

Show dataset profiles that would cover the following dataset:
Data set name . . . . . sysappl.cnracf.unload_____________________

Show profiles that would cover the following general resource name:
Resource class  . . . . ________
Resource name . . . . . ____________________________________________________
                        ____________________________________________________

Show members and profiles that would cover the following member resource:
Member class  . . . . . ________
Resource name . . . . . ____________________________________________________
                        ____________________________________________________


Display options used (change with "Setup View" or "Setup Confirm"):
access list SORT      - action commands EXECUTE   - confirm level ALL
```

Figure 149. Profile match selection panel

In the samples shown, all profiles that can protect the data set SYSAPPL.CNRACF.UNLOAD are selected. In this example, a data set name was specified, not a profile key.

The overview panel in the following figure shows the profiles that can match the data set. The profiles are sorted from specific to less specific. If the first profile is deleted, the second applies, and so on.

```
zSecure Suite Profile match                  1 s elapsed, 0.4 s CPU
 Command ===> ____________________________________________ Scroll===> CSR
 matching dataset SYSAPPL.CNRACF.UNLOAD          3 Mar 2001 00:07
    Profile key                                  T Complex  UACC    Owner    S/F
 __ SYSAPPL.CNRACF.**                            G TODAY    NONE___ SYSPROG_ __R
 __ SYSAPPL.**                                   G TODAY    NONE___ SYSPROG_ __R
 ****************************** BOTTOM OF DATA ********************************
```

Figure 150. Profile match overview display

By typing an S in front of a profile, the detail display, including the access list, is displayed. A sample detail display is included in the following figure..

```
zSecure Suite Profile match                                    Line 1 of 26
Command ===> _____________________________________________ Scroll===> CSR
matching dataset SYSAPPL.CNRACF.UNLOAD          3 Mar 2001 00:07
   Profile key                                  T Complex  UACC    Owner    S/F
   SYSAPPL.CNRACF.**                            G TODAY    NONE    SYSPROG    R
  User     Access  ACL id   When               Name                 InstData
_ -group-  READ___ C##GRACF PROGRAM_ CNARACF___                      PADS LIVE
_ -group-  READ___ C##GRACF PROGRAM_ CNRACF____                      PADS LIVE
_ -group-  ALTER__ SYSAPPL  ________ __________                      APPLICATIO
_ -group-  ALTER__ SYSPROG  ________ __________                      SYSTEM PRO
_ C##BJTI  READ___ C##BJTI  ________ __________ JOYCE TIMBERLINE
_ C##BJT2  READ___ C##BJT2  ________ __________ JOYCE TIMBERLINE
_ C##BNAT  READ___ C##BNAT  ________ __________ NICK THOMSON
_ C##BNA2  READ___ C##BNA2  ________ __________ NICK THOMSON
_ C##AUDIT READ___ C##AUDIT ________ __________ C/EPRISE AGENT       C/EPRISE A
```

Figure 151. Profile match detail display

The fields on the display panels are like the fields on a normal DATASET or RESOURCE display panel. However, the default sort order, the positioning of certain fields, and the amount of information included are different.

RA.3.8 GROUP TREE - Group tree display

Option **RA.3.8** provides an overview of the group structure of the system in a tree format. When you select this option, the Reports Group tree panel opens so you can specify selection criteria to select or exclude parts of the group structure.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - RACF - Reports Group tree
Command ===>                                                  _ start panel

Show structured group tree display:
Group id  . . . . . ________     (group profile key or filter)
Start at  . . . . . C##QA*__     (group or filter, show only groups below)
Scope of  . . . . . ________     (group special, show only groups in scope)
Exclude . . . . . . ________     (group or filter)
Complex . . . . . . ________     (complex name or filter)

Enter "/" to include data in output
 /  Installation data
 /  Users/Subgroups

Enter "/" to select option
_  Output in print format


'Start at' is only permitted with an unload as data source, not a live database
```

Figure 152. Report Group tree selection panel

The following selection criteria are supported:

Table 135. Group Tree Display - selection criteria

Selection criteria	Description
Group id	Group name or filter. Only matching groups are displayed
Start at	Only groups in the subtree with this group at the top is displayed. This type of selection is only supported for an UNLOAD.
Scope of	Show only groups in the scope of this user ID (meant for group special users)
Exclude	Group name or filter. Matching groups are not displayed
Complex	Name of complex name to show group tree for, or filter

In addition, the installation data of the groups shown can be included if desired, and (in display format only) the users connected to the groups, and the groups' subgroups can be shown on a detail display.

A sample group tree display is shown in the following figure.

```
zSecure Suite GROUP TREE DISPLAY                                Line 1 of 30
Command ===> ____________________________________________ Scroll===> CSR
                                        3 Mar 2001 00:07
   Complex  Groups
   TODAY        30
   Group structure                  Lvl Subgrp Connct SupGroup Owner    X
__      C##QA                         5      7    236 C##Q     C##Q
s_       C##BQAHW                     6      2      1 C##QA    C##BWTK  X
__         C##BQAHU                   7      0      0 C##BQAHW C##BQAHW
__         C##BQAH2                   7      0      1 C##BQAHW C##BWTK  X
__       C##BQALU                     6      0      1 C##QA    C##QA
__       C##BQAMC                     6      0     12 C##QA    C##QA
__       C##QA#HI                     6      0      0 C##QA    C##QA
__       C##QAT#1                     6      0      0 C##QA    R##SLIN  X
__       C##QDFPG                     6      1      0 C##QA    C##QA
__         C##QMWEG                   7      0      0 C##QDFPG C##QDFPG
__       C##QUNIX                     6      0      0 C##QA    C##QA
__      C##QA133                      5      0      0 C##Q     C##Q
__      C##QA134                      5      0      0 C##Q     C##Q
__      C##QA135                      5      0      0 C##Q     C##Q
__      C##QA136                      5      0      0 C##Q     C##Q
```

Figure 153. Report Group tree display

The following fields of interest are shown.

Table 136. Group Tree display fields

Field	Description
Complex	The complex name
Groups	The number of groups selected
Group structure	The groups, indented according to their depth in the group tree
Lvl	The group depth in the group tree
Subgrp	The number of subgroups for the group.
Connct	The number of connected users
SupGroup	The superior group for the group.
Owner	The owner for the group.
X	Indicates whether the superior group and owner are different.

Table 136. Group Tree display fields (continued)

Field	Description
Group	The group name (inclusion optional)
Installation data	The group installation data (inclusion optional)

When 'Users/Subgroups' has been selected, a detail display is available as shown in the following figure.

```
zSecure Admin GROUP TREE DISPLAY                              Line 1 of 24
Command ===>                                                   Scroll===> CSR
                                                  8 Feb 1999 00:05
   Group structure                          Lvl Subgrp Connct SupGroup Owner    X
        C##BQAHW                              6      2       2 C##QA    C##BWTK  X
  User     Auth    R SOA AG Uacc    Name                InstData
_ C##BWTK_ JOIN___ _ S__ _G ALTER__ WIGHT KENDALL
_ C##BBB1_ JOIN___ _ S__ _G ALTER__ BERNIE BAILEY
  SubGroup
_ C##BQAH2
_ C##BQAHU
******************************** BOTTOM OF DATA *********************************
```

Figure 154. Report Group tree detail display

For a further explanation, see the standard detail display for a group query ("RA.G GROUP - Group information" on page 117).

RA.3.9 USERDATA - User data management

Use option **RA.3.9** to find and view installation-defined User fields and change the `userdata`. When you select this option, the USERDATA selection panel shown in the following figure opens so you can specify the selection criteria to locate profiles.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - USERDATA selection
Command ===>

Specify selection criteria for USERDATA:
Class . . . . . ________
Profile . . . . . ________________________________________________________________
Complex . . . . . ________

Entry name  . . . . PHONE_____
Entry flag  . . . . __   (hexadecimal number, no filter)
Entry value . . . .
010*_____________________________________________________________________________


All fields but you can use the Entry flag field for either an exact match or a filter.
```

Figure 155. USERDATA selection panel

In the preceding example, we query for PHONE entries of which the contents starts with `010`.

The following selection criteria are supported.

Table 137. USERDATA - selection criteria

Field	Description
Class	The profile class, or filter.
Profile	The profile name, or filter.
Complex	The complex name, or filter.
Entry name	The name of the USERDATA entry, or a filter.
Entry flag	The USERDATA flag byte (hex).
Entry value	The value of the USERDATA entry, or filter.

This panel is not the intended interface to work with CKGRACF USERDATA entries. Therefore, entry names that start with *CKG* are suppressed unless you explicitly specify an **Entry name** starting with *CKG*.

The result of a query is a panel as shown in the following figure.

```
zSecure Admin Display Selection                  1 s elapsed, 0.3 s CPU
Command ===> ____________________________________________________ Scroll===> CSR

  Name     Summary Records Title
_ USERS          2       2 USERDATA values in user profiles
_ GROUPS         1       1 USERDATA values in group profiles
_ DATASET        1       1 USERDATA values in dataset profiles
_ RESOURCE       1       1 USERDATA values in general resource profiles
****************************** BOTTOM OF DATA ******************************
```

Figure 156. USERDATA overview

After selecting the results for USER profiles the following panel is shown.

```
USERDATA values in user profiles                                   Line 1 of 2
Command ===>                                                     Scroll===> CSR
                                              2 Nov 2001 00:05
   User     Name                 EntryNam Fl Value
s_ C##BGUS  GUS BAINES__________ <more>
__ C##BMCO  MATT CONNORS________ PHONE    00 01042703
****************************** BOTTOM OF DATA ********************************
```

Figure 157. USERDATA profile display

The other displays are similar in layout, but show the profile name under **Group** or **Profile key** instead of **User**, and have no **Name** field.

The following fields of interest are shown.

Table 138. USERDATA detail display

Field	Description
User	The profile name
Name	For users the programmer name
EntryNam	The USERDATA entry name
Fl	The USERDATA flag byte (hex)
Value	The USERDATA entry value

If there is only one (selected) USERDATA entry, it is shown on the profile display. If there are several entries, the listing shows the value <*more*>. The additional values are listed on the detail display panel. You can start the USERDATA management functions on the profile display with the **MU** line command. However, when you use this method, no entry information is passed to the command, and you have to enter the information manually. Therefore, for most management functions, it is easier to use the detail display.

A detail display is shown in the following figure.

```
USERDATA values in user
Command ===>                                                Scroll===> CSR
                                                  8 Feb 1999 00:05
   User     Name                 EntryNam Fl Value
   C##BGUS  GUS BAINES           <more>
  EntryNam Fl Value
r PHONE    00 0107823
_ PHONE    00 0102343
****************************** BOTTOM OF DATA ********************************
```

Figure 158. USERDATA values in user panel - detail display

The **D** Delete line command displays the following panel. You can optionally specify a reason when deleting an entry which consists of the name and value pair. For the **D** command, **Reason** is the only modifiable field.

```
                        Security zSecure - Delete USERDATA
Option ===>

Class . . . . . . . . USER____
Profile . . . . . . . 'ibmuser'c_____________________
Entry name  . . . . . PHONE___
Entry flag  . . . . . 00
Entry value . . . . . 0107823_____________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________
Reason
_____________________________________________________________________________
```

Figure 159. Delete USERDATA panel

The **R** Recreate line command creates another copy of the entry. The recreate option can be used to add another entry only if the command confirmation setting is turned on.

The **I** Insert, **C** Copy, and **S** Modify line commands bring up a panel to manage the `userdata`. The **C** and **S** commands result in a panel that provides all the values from the `userdata` entry. For the **I** command, only the Class and Profile data from the entry is included on the panel.

```
                        Security zSecure - Add USERDATA
Option ===>

Class . . . . . . . . USER____
Profile . . . . . . . 'ibmuser'c_____________________
Entry name  . . . . . PHONE___
Entry flag  . . . . . 00
Entry value . . . . . 0107823_____________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________
Reason
_____________________________________________________________________________
```

Figure 160. Add USERDATA panel

At the top the class and name of the profile you are working with is shown.

RA.3.A TAPEVOL - Tape Profile Overview

Option **RA.3.A** opens the Reports Tapevol panel, a variant of the General Resource Profiles panel that applies to the TAPEVOL class.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                         zSecure Suite - RACF - Reports Tapevol
Command ===>                                                  _ start panel

Show tape profiles that fit all of the following criteria:
Volume  . . . . . . ________     (tape volser or filter)
Owned by  . . . . . ________     (group or userid, or filter)
Complex . . . . . . ________     (complex name or filter)

 / Specify more selection criteria and output options



Display options used (change with "Setup View" or "Setup Confirm"):
user/grp info Y, action commands EXECUTE, confirm level ALL
```

Figure 161. TAPEVOL simple query panel

The simple query panel is shown in the preceding figure. The advanced selection panel is shown in the following figure.

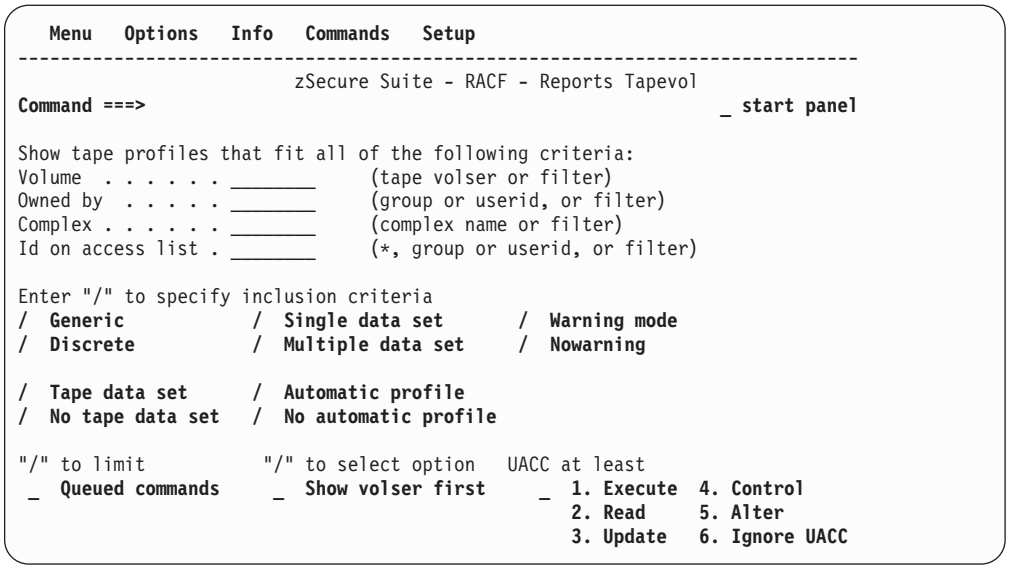


Figure 162. TAPEVOL advanced selection panel

The **Enter "/" to specify inclusion criteria** contains option pairs that are checked by default: Both generic and discrete profiles are shown based on the selection criteria specified on the Reports Tapevol panel. If you select options in the **"/" to limit** group, the selection is limited to only those profiles that possess the characteristics selected.

The following selection criteria are supported.

Table 139. Tapevol report - selection criteria

Selection criteria	Description
Volume	Tape volume occurring in the profile key or in the volume list.
Owned by	Profiles owned by the user or group you specified.
Complex	In a complex with this name, or a matching complex if a filter is used.
Id on access list	User or group on the access list (access that a user has through a group is *not* supported in this selection)
Generic	Show generic profiles.
Discrete	Show discrete profiles.
Single data set	Show profiles with single data set attribute.
Multiple data set	Show profiles without the single data set attribute.
Warning mode	Show profiles in Warning mode.
No Warning	Show profiles not in Warning mode.
Tape data set	Show profiles with tape data sets.
No tape data set	Show profiles without tape data sets.
Automatic profile	Show profiles with automatic attribute.
No automatic profile	Show profiles without the automatic attribute.
Queued commands	Show only groups that have one or more commands in the command queue.
UACC at least	Show any UACC that grants access greater than or equal to the specified value.

If you select the output option **Show volser first**, an overview of all volume serial names is presented first. Then, the profile data is listed per volume serial. If you do not select this option, the volume serial overview is not included.

A sample TAPEVOL profile display is shown in the following figure.

```
zSecure Admin TAPE OVERVIEW                                  Line 1 of 20
Command ===>                                                    Scroll===> CSR
All tape profiles                                    9 Feb 1999 00:05
  Profile  Complex  T UACC    Owner    Wrn #Vols Perms Conds SecLabel
__ CBM*     TODAY    G NONE___ SYSAUTH_ ___     0     4     0 ________
__ CNMASE   TODAY      NONE___ SYSAUTH_ ___     2     4     0 ________
__ CNV*     TODAY    G NONE___ SYSAUTH_ ___     0     4     0 ________
__ CPX*     TODAY    G NONE___ SYSAUTH_ ___     0     4     0 ________
__ CR2%%1   TODAY    G NONE___ SYSAUTH_ ___     0     5     0 ________
__ CR2*     TODAY    G NONE___ SYSAUTH_ ___     0     6     0 ________
__ CS2*     TODAY    G NONE___ SYSAUTH_ ___     0     5     0 ________
__ C4I*     TODAY    G NONE___ SYSAUTH_ ___     0     4     0 ________
__ C9%%%C   TODAY    G NONE___ SYSAUTH_ ___     0     3     0 ________
__ C9%%%R   TODAY    G NONE___ SYSAUTH_ ___     0     3     0 ________
__ GUUS01   TODAY      NONE___ C##BGUS_ ___     2     1     0 ________
s_ HSMHSM   TODAY      NONE___ SYSPROG_ ___   106     3     0 ________
__ PRTL*    TODAY    G NONE___ SYSAUTH_ ___     0     3     0 ________
__ PTFT*    TODAY    G NONE___ SYSAUTH_ ___     0     2     0 ________
__ QATAPE   TODAY      READ___ C##QARUN ___     1     3     0 ________
__ QATAP2   TODAY      NONE___ C##QARUN ___     1     3     0 ________
__ QATAP*   TODAY    G READ___ C##QARUN ___     0     4     0 ________
__ 003767   TODAY      NONE___ SYSAUTH_ ___     1     4     0 ________
__ 51665*   TODAY    G NONE___ SYSAUTH_ ___     0     2     0 ________
__ 520R*    TODAY    G NONE___ SYSAUTH_ ___     0     2     0 ________
****************************** BOTTOM OF DATA ******************************
```

Figure 163. TAPEVOL profile display

The following fields of interest are shown.

Table 140. Tapevol report panel - Show volser first output fields

Field	Description
Profile	The profile name
Complex	The complex name
T	The profile type: blank for discretes, or G for generics
UACC	Universal access level
Owner	The owner of the profile
Wrn	Warning attribute
#Vols	The number of volumes covered by the profile
Perms	The number of access list entries
Conds	The number of conditional access list entries
SecLabel	Security label

A detail display is shown in the following figure.

```
zSecure Admin TAPE OVERVIEW                                  Line 1 of 119
Command ===>                                                  Scroll===> CSR
All tape profiles                                  9 Feb 1999 00:05
   Profile  Complex  Type    UACC    Owner    Wrn #Vols Perms Conds SecLabel
   HSMHSM   TODAY            NONE    SYSPROG        106     3     0
  User     Access  ACL id   When                Name                 InstData
_ -group-  ALTER__ STGADMIN ________ __________                       STORAGE AD
_ -group-  ALTER__ SYSPROG_ ________ __________                       SYSTEM PRO
_ DFHSM    ALTER__ DFHSM___ ________ __________
  Volume
_ HSMHSM
_ 9BCK27
_ 9BCX24
_ 9BCL23
```

Figure 164. TAPEVOL detail display

Refer to "Access list display modes - reference material" on page 30 about alternate access list display formats.

RA.3.B RACFVARS - RACF variable profiles

Option **RA.3.B** shows the RACF Variable Profiles panel to select all RACFVARS profiles that fit the criteria listed.

```
   Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Reports RACFvars
Command ===>                                                  _ start panel

Show RACFVARS profiles that fit all of the following criteria:
Variable name . . . ________     (with leading &)
Member values . . . ____________________________________________ (list of values)
Owned by  . . . . . ________     (group or userid, or filter)
Complex . . . . . . ________     (complex name or filter)

/   Specify more selection criteria and output options


Display options used (change with "Setup View" or "Setup Confirm"):
user/grp info Y, action commands EXECUTE, confirm level ALL
```

Figure 165. RACFVARS simple query panel

The simple query panel is shown in the preceding figure. The advanced selection panel is shown in the following figure.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Reports RACFvars
Command ===>                                                  _ start panel

Show RACFVARS profiles that fit all of the following criteria:
Variable name . . . ________     (with leading &)
Member values . . . ____________________________________________ (list of values)
Owned by  . . . . . ________     (group or userid, or filter)
Complex . . . . . . ________     (complex name or filter)
Id on access list . ________     (*, group or userid, or filter)

Enter "/" to specify output option(s)
_  Show member names
_  View by duplicate entries
_  Sort member list
_  Show profiles that use Variable name
_  Output in print format
```

Figure 166. RACFVARS advanced selection panel

The following selection criteria are supported.

Selection criteria	Description
Variable name	Variable name matching the pattern.
Member values	Text strings that can appear anywhere in the member name. A pattern match is not supported (instead, a *substring scan* is always performed). If a list of values is specified, profiles are selected that contain any of the specified member names.
Owned by	Lists the OWNER you specified. The owner can be a user or group.
Complex	In a complex with this name, or a matching complex if a filter is used.
Id on access list	User or group on the access list (access that a user has through a group is *not* supported in this selection).

The following output options are available.

Table 141. RACF Variable Profile report - output options

Output option	Description
Show member names	Generate a display showing member names first, and show profiles that contain this member second.
View by duplicate entries	Generate a display showing only member names that appear in more than one RACFVARS profile.
Sort member list	Sort the member list. RACF determines matches by the *unsorted* member list, but always displays a sorted member list.
Show profiles that use Variable name	Include an extra display with profiles referring to a specific Variable name (requires the Variable name field to be filled in).
Output in print format	Generate output in printable format instead of in an ISPF table.

A sample RACFVARS overview panel is shown in the following figure.

```
zSecure Admin RACFVARS profile list              1 s elapsed, 0.2 s CPU
Command ===> _____________________________________________ Scroll===> CSR
All RACF variables                                 13 Jul 2005 00:07
   Profile  Complex  Members UACC    Owner    Wrn ID(*)   InstData
__ &C##A    DEFAULT        2 NONE___ R##PROB_ ___         ________________________
__ &C##AROB DEFAULT        3 NONE___ C##AROB_ ___         ________________________
__ &C##A1   DEFAULT        3 NONE___ R##PROB_ ___         ________________________
s_ &C##A2   DEFAULT        3 NONE___ R##PROB_ ___         ________________________
__ &C##NODE DEFAULT       26 NONE___ SYSPROG_ ___         ________________________
__ &LONGNAM DEFAULT        1 READ___ R##PROB_ ___         MAXIMUM LENGTH VARIAB
__ &RACLNDE DEFAULT       26 NONE___ SYSPROG_ ___         ________________________
__ &Z999999 DEFAULT        1 NONE___ C##BGUS_ ___         ________________________
****************************** Bottom of Data ********************************
```

Figure 167. RACFVARS overview display

A sample detail display is shown in the following figure.

```
zSecure Admin RACFVARS profile list                          Line 1 of 6
Command ===> _____________________________________________ Scroll===> CSR
All RACF variables                                 13 Jul 2005 00:07
   Profile  Complex  Members UACC    Owner    Wrn ID(*)   InstData
   &C##A2   DEFAULT        3 NONE    R##PROB
  User     Access  ACL id   When               Name                InstData
_ R##PROB  ALTER__ R##PROB_ ________ __________ RONNIE OBLIQUE
_ R##PRO2  ALTER__ R##PRO2_ ________ __________ RONNIE OBLIQUE
  Members
_ C##A_____________________________________
_ C##AINT__________________________________
_ C##ASCH__________________________________
****************************** Bottom of Data ********************************
```

Figure 168. RACFVARS detail display

RA.3.C APPL - Application profiles

Option **RA.3.C** generates a specially formatted overview of the profiles in the APPL class. Use the selection panel to specify whether you want the output in print format rather than as an ISPF table.

From the ISPF panel, you can specify action commands in the input entry field for each profile to work with the profile. To see a list of available actions, type / in an entry field, then press **Enter** for a list of the available commands.

A sample display is shown in Figure 169.

```
zSecure Admin Application profile overview       0 s elapsed, 0.2 s CPU
Command ===>                                                Scroll===> CSR
                                                  2 Feb 1999 15:25
    Complex  Class    Profile key      Type    Owner    UACC    InstData
__ DINO     APPL     #CNM                     SYSAUTH_ NONE___ NETVIEW_________
__ DINO     APPL     A21GTWOP                 SYSAUTH_ NONE___ ________________
__ DINO     APPL     A21RCPS1                 SYSAUTH_ NONE___ ________________
__ DINO     APPL     A21RUUFT                 SYSAUTH_ NONE___ ________________
__ DINO     APPL     CNM01                    SYSAUTH_ NONE___ NETVIEW_________
__ DINO     APPL     DINOLU01                 C##BMR1_ NONE___ ________________
__ DINO     APPL     ETPXLU01                 C##BMR1_ NONE___ ________________
__ DINO     APPL     NETVIEW                  SYSAUTH_ NONE___ NETVIEW_________
__ DINO     APPL     SYSPLU01                 C##BMR1_ NONE___ ________________
****************************** BOTTOM OF DATA ********************************
```

Figure 169. Application profiles overview

The detail display lists the access list entries.

RA.3.D JES/328X - Jes/328X definitions and log data sets

Option **RA.3.D** is a REPORT PROFILES variant designed to display JES328X queue authorities. The authority to issue JES328X commands or view the message log for specific printers is derived from the authority to either UPDATE or READ a log dataset existing for that remote terminal.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Reports - JES/328X
Command ===>

Data set pattern . . SYS1.JSXLOG.**                                (EGN mask)

Enter "/" to select option(s)
/  Include data sets in display
_  Output in print format
```

Figure 170. JES/328X selection panel

The following selection criteria and output options are supported.

Table 142. JES/328 definitions and log data sets - selection criteria and output options

Selection criteria or Output option	Description
Data set pattern	EGN specification of which DATASET profiles and data sets to show. This is set in the SETUP INSTALLATION application.
Include data sets in display	Indicates if the data sets covered by the profiles are to be included in the report
Output in print format	Generate output in print format instead of an ISPF display

A sample display is shown in the following figure.

```
Profiles used by JES/328X                              1 s elapsed, 0.6 s CPU
Command ===>                                                Scroll===> CSR
                                                  11 Feb 1999 09:40
   Complex  Class    Profiles
   RC223    DATASET         4
   Profile key                                    Volume UACC    S/F Era
__ SYS1.JSXLOG.*.**                                     READ___ __R NO_
__ SYS1.JSXLOG.RMT1                                     NONE___ __R NO_
__ SYS1.JSXLOG.RMT147                                   READ___ __R NO_
__ SYS1.JSXLOG.RMT148                                   NONE___ __R NO_
****************************** BOTTOM OF DATA ********************************
```

Figure 171. JES/328X detail display

The detail display also shows the same additional fields as the detail display of the PROFILES report. Because this is a REPORT PROFILES variant the line commands available are different from standard profile displays. See "RA.3.1 Profiles - Profiles with their data sets" on page 196.

RA.3.E SDSF - SDSF command and display authorities

Option **RA.3.E** generates an overview of all profiles that affect SDSF security. Use the selection panel to specify whether you want the output in print format rather than as an ISPF table.

A sample overview display is shown in following figure.

```
zSecure Admin Display Selection                1 s elapsed, 0.4 s CPU
Command ===>                                                Scroll===> CSR

  Name     Summary Records Title
_ GLOBAL         0       0 zSecure Admin SDSF control profiles
_ SDSF          33      33 zSecure Admin SDSF control of commands and inp
_ GSDSF          1       1 zSecure Admin SDSF grouping control of command
_ OPERCMDS      41      41 zSecure Admin SDSF control of MVS and JES2 com
_
****************************** BOTTOM OF DATA ********************************
```

Figure 172. SDSF resources overview display

Resources from four classes are shown:

Table 143. SDSF Security resource classes

Resource	Description
GLOBAL	Global access checking table entries for class SDSF
SDSF	Profiles protecting SDSF resources
GSDSF	Resource group profiles protecting SDSF resources
OPERCMDS	Profiles protecting operator commands

A profile display is shown in the following figure.

```
 zSecure Admin SDSF control of commands and input fields     Line 1 of 43
Command ===> ____________________________________________________ Scroll===> CSR
                                              15 Jul 2005 00:07
    Complex  Class Profile key                   T Owner    W UACC    ID(*)
__ TODAY    SDSF  **                           G SYS1____ _ NONE___
__ TODAY    SDSF  GROUP.*                      G SYS1____ _ NONE___ READ
__ TODAY    SDSF  ISFATTR.*.PRTY              G SYSPROG_ _ NONE___
__ TODAY    SDSF  ISFATTR.**                 G SYS1____ _ NONE___
__ TODAY    SDSF  ISFATTR.JOB.PRTDEST          SYSAUTH_ _ UPDATE_
```

Figure 173. SDSF profile display

On the detail display for SDSF, GSDSF and OPERCMDS the ACL entries are shown. For GSDSF and GLOBAL the member list is shown.

This option is a variant of **RA.R**, so see "RA.R RESOURCE - General Resource profiles" on page 147 for the available line commands.

RA.3.F JES2 - Access to JES2 resources

Option **RA.3.F** generates an overview of profiles that affect JES2 security. Use the selection panel to specify whether you want the output in print format rather than as an ISPF table.

A sample display is shown in the following figure.

```
zSecure Admin Display Selection                 1 s elapsed, 0.5 s CPU
Command ===>                                              Scroll===> CS

  Name     Summary Records Title
_ GLOBAL         2       2 zSecure Admin JES control profiles
_ JESINPUT       3       3 zSecure Admin JES input sources for job submis
_ FACILITY       2       2 zSecure Admin JES RACF validation of /*SIGNON
_ JESJOBS        1       1 zSecure Admin JES submit and cancel control
_ JESSPOOL      43      43 zSecure Admin JES sysin/sysout dataset access
_ NODES         12      12 zSecure Admin JES validation of inbound data c
_ WRITER         1       1 zSecure Admin JES outbound data control
_ PROPCNTL       0       0 zSecure Admin JES userid propagation control
_ SURROGAT      45      45 zSecure Admin JES surrogate submit control
****************************** BOTTOM OF DATA *******************************
```

Figure 174. JES2 resources overview display

Resources from these classes are shown:

Table 144. Display selection - class resources

Resource	Description
GLOBAL	Global access checking for JES control profiles
JESINPUT	JES input sources for job submission control
FACILITY	JES RACF validation of /*SIGNON and SNA LOGON
JESJOBS	JES submit and cancel control
JESSPOOL	JES sysin/sysout dataset access control
NODES	JES validation of inbound data control
WRITER	JES outbound data control
PROPCNTL	JES userid propagation control
SURROGAT	JES surrogate submit control

This option is a variant of **RA.R**.

RA.3.G Compare users - Compare access and/or connect

Use this option to do the following comparisons:

- Compare access through permits with an option to include group permits.
- Compare connects for up to four userids

When you select RA.3.G, the following panel opens:

```
   Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - Reports - Compare
Command ===> ____________________________________________________________________

Enter up to 4 userids to compare access and/or connects
Userid  . . . . SECADM1_     SECADM2_     ________     ________

Select report(s)
_  Compare access through user-specific permits
   _  Include group permits
_  Compare connects
```

Figure 175. Compare selection panel

Table 145 lists the available selection criteria and output options

Table 145. Compare selection - selection criteria

Selection criteria	Description
Userid	Enter up to 4 user IDs to compare. Masks are not permitted.
Compare access through user-specific permits	Compare access through an explicit permit for the user IDs entered.
Include group permits	This option is only effective when **Compare access through user-specific permits** is selected as well. The generated report also displays access through group connects.
Compare connects	Compare the group connects for the user IDs entered.

Figure 176 shows the panel that is displayed when all options are selected:

```
zSecure Suite Display Selection                                  Line 1 of 2
Command ===> ____________________________________________________ Scroll===> CSR_
   Name     Summary Records Title
_ PERMIT        31    3420 Compare PERMITs for users, including group permits
_ CONNECT       17      17 Compare CONNECTs for users
****************************** Bottom of Data ********************************
```

Figure 176. PERMIT/CONNECT summary panel

Selecting the PERMIT entry opens the overview panel shown in Figure 177.

```
Compare PERMITs for users, including group permits               Line 1 of 31
Command ===> ____________________________________________________ Scroll===> CSR_
Enter S in front of a class for more info                    10 Feb 2006 09:51
   Class    Profiles SECADM1 SECADM2
__ APPCLU          2 ALTER   NONE
__ APPL            3 READ    READ
__ CONSOLE         3 ALTER   NONE
__ CSFKEYS         1 READ    NONE
__ CSFSERV         1 READ    NONE
__ DASDVOL         2 ALTER   NONE
__ DATASET      1471 ALTER   ALTER
__ DLFCLASS        1 ALTER   NONE
__ EJBROLE         1 READ    READ
__ FACILITY      326 ALTER   ALTER
__ FIELD          22 ALTER   READ
__ GCICSTRN        5 ALTER   NONE
__ IBMOPC          3 READ    READ
__ JESSPOOL       39 ALTER   ALTER
__ NETCMDS         2 UPDATE  NONE
__ NETSPAN         1 UPDATE  NONE
__ OPERCMDS       54 ALTER   UPDATE
__ PROGRAM        13 ALTER   ALTER
__ RACFVARS        2 ALTER   NONE
__ RRSFDATA        8 ALTER   READ
```

Figure 177. PERMIT class overview panel

In Figure 178 on page 232, you see the RACF class, the number of profiles within this class that have permits for any of the user IDs specified in the selection criteria and the highest access within this class for these user IDs.

Figure 178 on page 232 When you select a class entry, the profiles within this class are displayed as shown in Figure 178 on page 232.

```
Compare PERMITs for users, including group permits                Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR_
Enter S in front of a class for more info                   10 Feb 2006 09:51
   Class    Profiles SECADM1 SECADM2
   APPCLU          2 ALTER   NONE
   Profile key                                  SECADM1 SECADM2
__ NLCRMM04.APR2001.NLCRMM04.R#MVS522           ALTER   NONE
__ NLCRMM04.RRSFCRM4.NLCRMM04.R#MVS522          ALTER   NONE
****************************** Bottom of Data ********************************
```

Figure 178. PERMIT profile overview panel

You can select a profile for more details about the access:

```
Compare PERMITs for users, including group permits                Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR_
                                             10 Feb 2006 09:51
   Class    Profiles SECADM1 SECADM2
   APPCLU          2 ALTER   NONE
   Profile key                                  SECADM1 SECADM2
   NLCRMM04.APR2001.NLCRMM04.R#MVS522           ALTER   NONE
   Scope of Access  Via      When
__ SECADM1  ALTER   SECADMG
****************************** Bottom of Data ********************************
```

Figure 179. PERMIT profile overview panel

In Figure 179, user ID SECADM1 has ALTER access to this profile as a result of a CONNECT to group SECADMG. To view the full profile name that SECADM1 has access to, select the SECADM1 entry. Then, press Enter.

When you select the CONNECT entry (see Figure 176 on page 231), the overview panel shown in Figure 180 is displayed.

```
Compare CONNECTs for users                                       Line 1 of 17
Command ===> _____________________________________________ Scroll===> CSR_
Enter S in front of a group to change connect               10 Feb 2006 10:17
   Group    SECADM1  SECADM2
__ CRBEHEER Yes      No
__ CRM      No       Yes
__ CRMB     Yes      Yes
__ CRMBEPRD No       Yes
__ CRMBMR   No       Yes
__ CRMBOMVS Yes      No
__ CRMBQA   Yes      No
__ CRMBRACF Yes      Yes
__ CRMBREAD Yes      Yes
__ CRMBZDEV Yes      Yes
__ CRMCNG   Yes      Yes
__ CRMGRACF Yes      Yes
__ DSNADBA  Yes      No
__ DSNASYS  Yes      No
__ FWGRP    Yes      No
__ STGADMIN Yes      No
__ SYSPROG  Yes      No
****************************** Bottom of Data ********************************
```

Figure 180. CONNECT group overview panel

The columns show the group name and whether the user ID is connected to this group.

When you select a group entry, the Connects are shown.

```
Compare CONNECTs for users                                      Line 1 of 6
Command ===> _____________________________________________ Scroll===> CSR_
                                          10 Feb 2006 10:17
   Group
   CRBEHEER
  User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt
_ SECADM1  USE              NONE
_ CNM01PPT USE              NONE
_ CNMCSSIR USE              NONE
_ AUTO3    USE              NONE
_ AUTO2    USE              NONE
_ AUTO1    USE              NONE
****************************** Bottom of Data ********************************
```

Figure 181. CONNECT detail display

RA.4 MASS UPDATE - Specify mass copy/recreate/delete actions

The MASS UPDATE application provides an easy way to change, add, or delete multiple profiles in one run. The functions provided are the same as the functions available from the corresponding line commands. However, the MASS UPDATE update function permits you to run these commands on multiple profiles.

The MASS UPDATE application is an advanced function for experienced security administrators who understand the impact of their selections and actions.

```
  Menu   Options   Info   Commands   Setup   StartPanel
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Mass update
Option  ===> ____________________________________________

0    Copy user       Copy existing user(s) to new user(s)
1    Copy group      Copy existing group(s) to new group(s)
2    Copy dataset    Copy dataset profile(s) to another high level qualifier
3    Copy resource   Copy general resource profile(s) to another class
4    Delete user     Delete user(s)
5    Delete group    Delete group(s)
6    Recreate user   Recreate user(s)
7    Recreate grp    Recreate group(s)
8    Recreate ds     Recreate dataset profile(s)
9    Recreate res    Recreate general resource profile(s)
C    Copy CICS       Copy CICS prefixed profile(s) or member(s)
```

Figure 182. Mass update menu

Use the COPY options to specify several profiles of the selected type that must be created like an existing profile. Copying is also called *cloning*.

Use the DELETE options to perform daily maintenance functions for the user entry staff. These options generate commands to delete user or group profiles and all references to the IDs from the RACF database. Specify commas before a value if you also want to remove all the data sets covered by the removed profiles, including cataloged data sets migrated (volume `MIGRAT` or `ARCIVE`) to tape, but excluding migrated-but-uncataloged and true tape data sets. If you do not supply a `CKFREEZE` file, resource deletion is automatically skipped. For information on the REMOVE command, see "REMOVE" on page 870.

The RECREATE options are designed to generate commands from a RACF database that can be used for rebuilding selected profiles as they exist in that database. For example, you can use the RECREATE option after a profile has been inadvertently deleted. To reinstate the profile, restore the RACF database form last week, and then define an input set containing these data sets as described in “SE SETUP - Options and input data sets used” on page 1641. You can then run any report against the old database, and use RECREATE to generate RACF commands for the profiles you lost.

You can also use RECREATE to generate RACF commands that you manipulate with the editor to create a COPY routine.

RA.4.0 Copy user - Copy an existing user to a new user

Use option **RA.4.0** to create, or clone several user profiles from one or more model user profiles at the same time. Figure 183 shows the User Multiple copy panel for performing these tasks.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                         zSecure Suite - RACF - User Multiple copy
Command ===>

Create new user(s) like existing user(s):
_  Specify password phrases

Model    New
User     User     Password Name                 Owner    Dfltgrp  Data
c##bjti_ c##bjt3_ JJW_____ JOYCE_TIMBERLINE____ c##bjti_ c##b____ _________
=_______ c##bjt4_ =_______ =____________________ =_______ =_______ _________
c##bjt2_ c##bjt5_ =_______ =____________________ =_______ =_______ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________
________ ________ ________ ____________________ ________ ________ _________

Enter = to copy value from preceding line, leave blank to copy from model.

Press ENTER to specify optional parameters.
```

Figure 183. User Multiple copy panel

On each line, specify the existing user that provides the model to copy from, the new user to create, and any characteristics that are not to be copied from the model user. In the following lines, you can specify = to use the same value used on the preceding line.

If the new user must be a protected user ID, enter * as password.

If you select **Specify password phrases**, a follow-up panel is shown for setting password phrases for the new user IDs. This option cannot be combined with entering a * (for protected) for all new users.

When you press **ENTER** on the User Multiple copy panel, the = markers are replaced by repetitions from the preceding lines, as shown in Figure 184 on page 235.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                zSecure Suite - RACF -          Default prompting
Command ===>

Create new user(s) like existing user(s):
_  Specify password phrases
Model    New
User     User     Password Name                 Owner    Dfltgrp  Data
C##BJTI_ C##BJT3_ JJW_____ JOYCE_TIMBERLINE____ C##BJTI_ C##B____ ______
C##BJTI_ C##BJT4_ JJW_____ JOYCE_TIMBERLINE____ C##BJTI_ C##B____ ______
C##BJT2_ C##BJT5_ JJW_____ JOYCE_TIMBERLINE____ C##BJTI_ C##B____ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______
________ ________ ________ ____________________ ________ ________ ______

Enter = to copy value from preceding line, leave blank to copy from model.

Press ENTER to specify optional parameters.
```

Figure 184. User Multiple copy panel - user selection

When you press **Enter** again, the panel shown in Figure 185 opens.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                      zSecure Suite - RACF - User Multiple copy
Command ===> ____________________________________________________________

Optional parameters
Do not connect new user(s) to following group(s):
________  ________  ________  ________  ________
________  ________  ________  ________  ________
Also connect new user(s) to following group(s):
________  ________  ________  ________  ________
________  ________  ________  ________  ________

 _  Generate RACF commands even when the target user exists
 _  Copy USERDATA and CUSTOMDATA

Specify options for new userid
_  Revoke new userid
/  Copy catalog aliases (only if CKFREEZE is present)
_  Issue ADDSD/RDEF for dataset and resource profiles related to the user
   /  Copy RACFVARS profiles/members too

Press ENTER to generate TSO and RACF commands.
```

Figure 185. User Multiple copy panel

Optionally, you can specify groups that users cannot connect to even though the model user is connected. You can also specify groups that the user can connect to. Selecting the **Generate RACF commands** option when the target user exists forces the program to generate commands even though the user exists.

When you select **Copy USERDATA and CUSTOMDATA**, CKGRACF commands are generated to copy the user data. RACF commands are also generated to copy custom fields. You can also specify the following options:

- Make new users revoked initially to prevent default passwords from being available.

- Whether to clone catalog aliases.
- Whether to clone user-specific data sets and general resource profiles like STARTED and SURROGAT profiles.

  If they are cloned, you can indicate whether the RACFVARS profiles also require cloning.

Note: By default, the occurrence of a valid user ID as a member or the key of a RACFVARS profile is considered meaningful, although RACF itself assigns no special meaning to this occurrence..

After specifying all the criteria, press **Enter** to generate the applicable RACF and TSO commands. The results are shown in an edit panel showing the CKRCMD file.

RA.4.1 Copy group - Copy existing groups to new groups

Use option **RA.4.1** Copy group to create (or *clone*) several groups from one group at the same time. The panel presented for this purpose is shown in the following figure.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - Mass update - Copy group
Command ===> ____________________________________________________________

From group  . . . . ________
To id . . . . . . . ________ ________ ________ ________ ________
                    ________ ________ ________ ________ ________

_  Copy permits only (target id may be a group or a user)
_  Generate RACF commands even when the target group exists
_  Copy CUSTOMDATA

Specify options for new group:
_  Copy catalog aliases (only if CKFREEZE is present)
_  Issue ADDSD/RDEF for user resources
  _  Copy RACFVARS profiles/members too (if option above selected)
```

Figure 186. Group multiple copy panel

Optionally, you can suppress the error message indicating that the new group ID exists. The suppress command effectively adds connections and permits of the model group to the target groups. By selecting **Copy permits only**, you indicate that the permits of the model group are to be added to the target groups or users. No CONNECT or ADDGROUP commands are generated.

When the **Copy CUSTOMDATA** option is selected, RACF commands are generated to copy custom fields. You can also specify whether catalog aliases are to be cloned and whether group-specific data sets and general resource profiles are to be cloned as well. If these profiles are cloned, then you can also specify whether the RACFVARS profiles are also to be cloned.

Note: By default the occurrence of a valid group ID as a member or the key of a RACFVARS profile is considered meaningful, although RACF itself assigns no special meaning to this occurrence.

After completing this panel, press **Enter** to generate the applicable RACF and TSO commands. The generated commands are shown in an edit panel showing the CKRCMD file.

RA.4.2 Copy dataset - Copy dataset profiles to another High-level qualifier

Use option **RA.4.2** Copy dataset to copy DATASET profiles with a specific High-level qualifier to another HLQ.

```
   Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - Data set Multi-Copy
Command ===>

Copy dataset profiles that match the following high qualifier:

Dataset HLQ . . . . C##BJTI_


To qualifier  . . . C##BJT3_


This function is not available in restricted mode
```

Figure 187. Dataset multiple copy panel

In this panel you specify the **Dataset HLQ** for which profiles are to be copied, and the qualifier they are to be copied to. This destination qualifier is not verified to see if it is a valid user or group, even though the generated commands fail if the user or group is not valid.

This might result in output as shown in the following figure.

```
EDIT       C##BJTI.C2R1EF2A.CKRCMD                        Columns 00001 00072
Command ===>                                                 Scroll ===> CSR
Press PF3, enter R at the cursor location, press ENTER to run these commands
000001         /* CKRCMD file CKR1CMD complex DINO NJE JES2DINO generated  3 No
000002          /* Commands generated by COPY PERMIT       */
000003         addsd 'C##BJT3.**' generic from('C##BJTI.**') fgeneric
000004         addsd 'C##BJT3.RE.DUN.DANT.**' generic from('C##BJTI.RE.DUN.DANT
000005         altdsd 'C##BJT3.**' generic owner(C##BJT3 )
000006         altdsd 'C##BJT3.RE.DUN.DANT.**' generic owner(C##BJT3 )
000007         SETROPTS REFRESH GENERIC(DATASET)
****** ***************************** Bottom of Data ****************************
```

Figure 188. Dataset multiple copy commands

After reviewing the commands, and altering them as desired, PF3 exits the panel and returns you to the RESULTS panel where you can specify **R** Run in front of the CKRCMD file to run the commands.

RA.4.3 Copy resource - Copy general resource profiles to another class

Use option **RA.4.3 Copy resource** to copy general resource profiles (matching a pattern) from one class to another. Make sure to specify an existing class as the destination because the program does not check the class value. If you specify an invalid class, the generated commands fail when they are run.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Multi-Copy
Command ===>

Copy general profiles that fit all of the following criteria:
Class name  . . . . GCICSTRN     (class or filter)
Profile pattern . . **_____________________________________________ (EGN mask)

To class  . . . . . GCIC2TRN
```

Figure 189. Resource multiple copy panel

In the preceding example, all profiles in the GCICSTRN class are copied to class GCIC2TRN.

RA.4.4 Delete user - Delete users

Use option **RA.4.4 Delete user** to delete or remove user IDs, connections, and permissions. Depending on the options you select, you can generate the following types of delete and remove commands which you can edit and submit for processing:

- Delete multiple user IDs.
- Move these user IDs to a different holding group.
- Remove only permits.
- Remove users from the NOTIFY fields.

You can generate the commands to process up to 12 user IDs at one time.

```
    Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                           zSecure Suite - RACF - User Delete
Command ===>

Userid  . . . . . . ________ ________ ________ ________ _______ ________
                    ________ ________ ________ ________ _______ ________
Specify action to perform
_  1. Delete userid
   2. Move userid to holding group ________
   3. Remove userid from resource profiles (remove permit)
   4. Remove userid from NOTIFY fields

Specify resources to delete (actions 1, 2 and 3 only)
/  Data set and id-specific profiles
   Only if previous option selected:
   _  RACFVARS profiles and members
   /  Data sets and their catalog entries
      /  Incl. catalog entries without data sets
      /  Incl. uncataloged data sets

Change USERID in Notify fields to   ________  (default is NONOTIFY)
New Owner for non-dataset profiles  SYS1____  (default is SYS1)
```

Figure 190. User multiple delete panel

Enter the user IDs to be processed in the **Userid** field. Then, choose the action to be performed.

1 Delete userid. Deletes the user ID and all references and profiles solely in use for that user. This action generates the following command: REMOVE USER=*id*. command. refer to “REMOVE” on page 870.

2 Move userid to a holding group. Revokes the user ID, deletes the user ID current connections, and connects it to the specified holding group. This action generates the following command: REMOVE USER=*id* TOGROUP=*group* REVOKE.

3 Remove userid from resource profiles Removes the user ID from the resource profile without deleting the user ID connections or the profile itself. This action generates the following command: REMOVE NOTIFY=*id*.(REMOVE PERMIT=*id*).

4 Remove userid from NOTIFY fields Only deletes the user ID from NOTIFY fields. This action generates the following command: REMOVE NOTIFY=*id*.

The options control to what extent delete commands are generated:

Dataset and id-specific profiles
Deletes ID-specific profiles. If this option is not selected, the removal of user-specific profiles is suppressed, and data sets are kept. Deleting a user ID fails if the user ID is associated with any of the remaining data set profiles.

RACFVARS profiles and members

Security zSecure expects that the occurrence of a valid user ID as a key preceded by an ampersand (*&userid*) or a member of a RACFVARS profile to be meaningful. As a result, if you select the option, the profile or profile member is removed accordingly.

Datasets and their catalog entries
When you select this option and a CKFREEZE file has been allocated, the deletion of profiles is preceded by the deletion of the data sets covered by them. This means that unprotected or inaccessible data sets with an HLQ that matches the removed ID are also removed.

This option also deletes catalog entries based on the following option settings:

- If **Incl. Catalog entries without datasets** is selected, the entries deleted depend on the DELETE NOSCRATCH option setting when necessary.
- If **Incl. Uncataloged data sets** is selected, uncataloged non-VSAM data sets from the VTOC are scratched.

See “SUPPRESS” on page 932 for more information about the effect of delete operations when volumes or catalogs are explicitly excluded, or when they are implicitly excluded by not supplying enough `CKFREEZE` files for the analysis as can happen with partially shared DASD, . Resource deletion commands are explicitly targeted at the current system. If you must run additional resource deletion commands from another system, do not forget to update your `CKFREEZE` files.

You can also specify a replacement for the occurrence of the user in `NOTIFY` and `OWNER` fields. The default behavior is to delete NOTIFYs and replace `OWNER`s by *SYS1*.

RA.4.5 Delete group - Delete groups

Use option **RA.4.5 Delete group** to generate the commands to delete multiple groups or to only remove the permits. You can generate the commands to process up to 12 user IDs at one time.

Resource deletion commands are explicitly targeted at the current system. If you need to run additional resource deletion commands from another one, do not forget to update your CKFREEZE files.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Suite - RACF - Group Delete
Command ===>

Group . . . . . . . ________ ________ ________ ________ ________ ________
                    ________ ________ ________ ________ ________ ________

Specify action to perform
 _  1. Delete group
    2. Remove group from resource profiles (remove permit)

Options for delete group                          Options for connected users
Enter "/" to select option(s)                     Delete all USERs ...
 /  Dataset and id-specific profiles                /  owned by GROUP
    Only if previous is selected:                   _  connected to GROUP
    _  RACFVARS profiles and members                _  with defaultgrp GROUP
    /  Data sets and their catalog entries         Or move USERs to holding
       /  Incl. catalog entries without data sets            group ________
       /  Incl. uncataloged data sets

Change USERID in Notify fields to   NONOTIFY  (default is NONOTIFY)
New Owner for non-dataset profiles  SYS1____  (default is SYS1)
```

Figure 191. Group multiple delete panel

Enter the groups to be processed in the **Group** field, and choose the action to be performed.

1 Delete groupid. Deletes the group ID and all references and profiles solely in use for that group. This action generates the following command: `REMOVE GROUP=id`.

2 Remove groupid from resource profiles Deletes the group permissions without deleting the group. This action generates the following command: `REMOVE PERMIT=id`.

For information on the REMOVE commands, see "REMOVE" on page 870.

The options control to what extent delete commands are generated:

Dataset and id-specific profiles
Deletes ID-specific profiles. If this option is not selected, the removal of group-specific profiles is suppressed, and data sets are kept. Deleting a group ID fails if the group ID is associated with any of the remaining data set profiles.

RACFVARS profiles and members

Security zSecure expects that the occurrence of a valid group ID as a key preceded by an ampersand (*&groupid*) or a member of a RACFVARS profile to be meaningful. As a result, if you select the option, the profile or profile member is removed accordingly.

Datasets and their catalog entries
When you select this option and a `CKFREEZE` file has been allocated, the deletion of profiles is preceded by the deletion of the data sets covered by them. This processing behavior means that unprotected or inaccessible data sets with an HLQ that matches the removed ID are also removed.

This option also deletes catalog entries based on the following option settings:

- If **Incl. Catalog entries without datasets** is selected, the entries deleted depend on the DELETE NOSCRATCH option setting when necessary.
- If **Incl. Uncataloged data sets** is selected, uncataloged non-VSAM data sets from the VTOC are scratched.

See “SUPPRESS” on page 932 for more information about the effect of delete operations when volumes or catalogs are explicitly excluded, or when they are implicitly excluded by not supplying enough CKFREEZE files for the analysis as can happen with partially shared DASD. Resource deletion commands are explicitly targeted at the current system. If you must run additional resource deletion commands from another system, do not forget to update your CKFREEZE files.

A simple group deletion only works if the group does not contain any users. For that reason the panel offers the options to delete users owned by the group, connected to the group, or having the group as default group. You also have the option to remove the users from the group by revoking the user IDs and moving them to a holding group.

You can also specify a replacement for the occurrence of the group in NOTIFY and OWNER fields. The default behavior is to delete NOTIFY statements and replace OWNERs values with *SYS1*.

RA.4.6 Recreate user - Recreate users

Use the Recreate user option (**RA.4.6**) to generate commands to recreate one or more user IDs.

You can also edit the generated commands to copy the user ID instead of recreating it. This type of copy is useful if you already have permits for users like ADGRANT, ADGRANT1 and want to add permits for COPGRANT, COPGRAN1.

Although you can use an UNLOAD file as the input for the RECREATE USER command, the recreated profile can be incomplete or wrong because the user information in the UNLOAD file is not current. Also, in the UNLOAD file all sensitive fields like password and password phrase are always created with a mask ********.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Recreate
 Command ===>

Recreate userid . . ________     (user profile key or filter)
Owner . . . . . . . ________     (group or userid, or filter)

Specify options for recreate
/  Copy Dataset and General Resource profiles for this user
/  Copy Access List entries with this user
/  Use CKGRACF to update the user profile
```

Figure 192. User Recreate panel

.

The following selection criteria are available.

Table 146. Recreate user - selection criteria

Selection criteria	Description
Recreate userid	The user ID to be recreated, or a filter
Owner	The owner of the user IDs to be recreated, or a filter

If you want the user IDs DATASET and General Resource profiles to be recreated as well, select the **Copy Dataset and General Resource profiles for this user**

recreate option. If you want the user ID to be reinstated with PERMITs on profile access lists, select **Copy Access List entries with this user**. If you select this option, you can also select the **Use CKGRACF to update the user profile** setting to generate the CKGRACF commands to restore additional information, USERDATA and CKGRACF data for example.

The user that is running the generated CKGRACF commands must have sufficient access for running these commands, and the users to be defined must be in the user's CKGRACF scope. The use of the CKGRACF FIELD command is not subject to scope checks. See "CKGRACF authority checks" on page 1559.

RA.4.7 Recreate grp - Recreate groups

User option **RA.4.7 Recreate group** to generate commands to recreate one or more groups.

You can also edit the generated commands to copy the group ID instead of recreating it. This type of copy is useful if you already have permits for groups like *SYS1R*, *SYS1U* and want to add permits for SYS9R, SYS9U

RECREATE can also be used to copy profiles. After you run the command, you can edit the resulting commands to specify the name of the profile to copy to. This operation can be an effective copy method if you already have permits for groups and want to add permits for SYS9R, SYS9U, and so on.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Group Recreate
 Command ===>

Recreate groupid  . ________     (group profile key or filter)
Owner . . . . . . . ________     (group or userid or filter)

Specify options for recreate
_  Copy Dataset and General Resource profiles for this group
/  Copy Access List entries with this group /  Use CKGRACF to update the group profile
```

Figure 193. Group recreate panel

The following selection criteria are available.

Table 147. Recreate group - selection criteria

Selection criteria	Description
Recreate groupid	The group to be recreated, or a filter
Owner	The owner of the groups to be recreated, or a filter

If you want the DATASET and General Resource profiles for the group to be recreated as well, select the first option. If you want the group to be reinstated with PERMIT statements on profile access lists, select the second option. Select the third option to generate CKGRACF commands to restore additional information like USERDATA and CKGRACF data.

RA.4.8 Recreate ds- Recreate data set profiles

Option **RA.4.8 Recreate dataset** can be used to generate commands to recreate one or more data set profiles.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Data set Recreate
Command ===>

Profile pattern . . _____________________________________________ / EGN mask
Qualifier . . . . . ________     (or filter as modified by ICHCNX00)
Owner . . . . . . . ________     (group or userid or filter)

Specify options for recreate
```

Figure 194. Data set Recreate panel

The following selection criteria are supported.

Table 148. Recreate data set profile - selection criteria

Selection criteria	Description
Profile pattern	The *name* of the profile to be recreated if the **EGN mask** option is unchecked, otherwise a *filter*
EGN mask	Whether to interpret the profile patterns specified as a filter rather than a name
Qualifier	The High-level qualifier of the profile (as modified by ICHCNX00 if present), or a filter
Owner	The owner of the profiles to be recreated, or a filter

Select the **Use CKGRACF** option to generate CKGRACF commands to restore additional information like USERDATA and CKGRACF data.

RA.4.9 Recreate res - Recreate general resource profiles

Option **RA.4.9 Recreate resource** can be used to generate commands to recreate one or more general resource profiles.

Although you can use an UNLOAD file as the data source for RECREATE operations, doing so can result in incorrect information because any masked or confidential fields included in the data are not recreated properly.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - Resource Recreate
Command ===> _____________________________________________________________

Recreate class  . . ________      (class or filter)
Profile pattern . . ____________________________________________ / (EGN mask)
Owner . . . . . .   ________
Search  . . . . .   ____________________________________________________________
____________________________________________________________________________

Specify options for recreate
/  Use CKGRACF to update the general resource profile
```

Figure 195. Resource Recreate panel

The following selection criteria are available.

Table 149. Recreate general resource profiles - selection criteria

Selection criteria	Description
Recreate class	The class to recreate profiles from, or a filter

Table 149. Recreate general resource profiles - selection criteria (continued)

Selection criteria	Description
Profile pattern	The *name* of the profile to be recreated if the **EGN mask** option is unchecked, otherwise a *filter*
EGN mask	Whether to interpret the profile patterns specified as a filter rather than a name
Owner	The owner of the profiles to be recreated, or a filter
Search	Text strings to search for anywhere in the profile

Select the **Use CKGRACF** option to also generate `CKGRACF` commands to restore additional information, `USERDATA` and `CKGRACF` data for example.

Currently, the classes UNIXMAP, DIGTNMAP, DIGTCERT and DIGTRING are not supported here.

RA.4.C Copy CICS - Copy CICS prefixed profiles or members

You can use Option **RA.4.C** Copy CICS for copying CICS prefixed profiles, or CICS prefixed members of grouping classes. The panel presented for this purpose is shown in the following figure.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Suite - RACF - Copy CICS
Command ===> ____________________________________________________________

Class  . . . . . . . _________  (CICS resource class)
Profile pattern  . . ____________________________________________  (EGN MASK)
From CICS prefix . . _________  (Source CICS userid when grouping class)

To CICS prefix . . . _________  (CICS userid for prefixing new profile(s))
```

Figure 196. Copy CICS prefixed profiles panel

The following selection criteria are supported.

Table 150. CICS profiles, members, or grouping classes - selection criteria

Selection criteria	Description
Class	The CICS resource class, or a filter. This field is a required input field.
Profile pattern	The CICS profile name, or a filter. This field is a required input field.
From CICS prefix	The CICS source `userid`. This value is the profile High-level qualifier, or member prefix for grouping classes.
To CICS prefix	The target CICS `userid`. Commands are generated to add a new profile that uses this ID as the High-level qualifier, or add members to the CICS profiles for grouping classes.

RA.5 DIGTCERT - Work with digital certificates

The menu option RA.5 (DIGTCERT) can be used to select digital certificates.

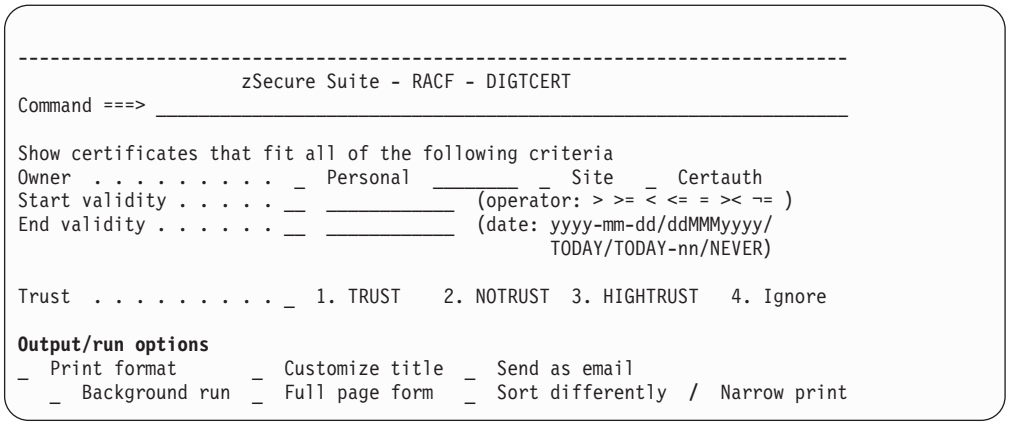


Figure 197. DIGTCERT selection panel

The following selection criteria are available:

Table 151. Digital Certificate reporting- available selection criteria

Selection criteria	Description
Owner	Select certificates for one or more user IDs (PERSONAL), all certificate-authority certificates (CERTAUTH), or all site certificates (SITE). For PERSONAL certificates, you can optionally use filters to select certificates for multiple userids. You can use the percent symbol (%) to select one character and you can use the asterisk symbol (*) to select zero or more characters.
Start validity operator	Use the operator to determine the date for selection. Use < and <= for selection prior to or on the date specified, > or >= for later dates, = for exact dates, ¬= or <> for all but the specified date.
Start validity	The start of the validity of the digital certificates. The date can be specified as: *ddmmmyyyy*, *01jan1998* for example. *yyyy-mm-dd*, *1998-01-01* for example. *TODAY* TODAY-*xx* or TODAY+*xx*where *xx* is a number of days. *NEVER* to indicate that no start validity date has been set.
End validity operator	Use the operator to determine the date for selection. Use < and <= for selection prior to or on the date specified, > or >= for later dates, = for exact dates, ¬= or <> for all but the specified date.
End validity	The end of the validity of the digital certificates. The date can be specified as: *ddmmmyyyy*, *01jan1998* for example. *yyyy-mm-dd*, *1998-01-01* for example. *TODAY* TODAY-*xx* or TODAY+*xx*where *xx* is a number of days. *NEVER* to indicate that no end validity date has been set.
Trust	Selects certificates based on their trusted status.

Table 151. Digital Certificate reporting- available selection criteria (continued)

Selection criteria	Description
CERTAUTH, MULTIID, SITE	Report or suppress CERTAUTH, MULTIID, and SITE certificates. Specify `Y` to only report these certificates, `N` to suppress them, or blank to report all certificates.
Userid	Selects on the user ID associated with a certificate. You can use the following filters to select more than one user ID: `%` for one character and `*` for one or more characters.

You can select the following output and run options by entering / or *S* in the input field for the option.

Table 152. Digital Certificate reporting - output and run options

Option	Description
Print format	If this field is selected, the output data is formatted for printing rather than for ISPF display. When you select this option, other print-related options become active for further customization of the printed report. This flag setting is saved in your ISPF profile and is shared between all RA options showing it. The print format is either tabular or form-oriented. You can select the **Full page form** option if you want the results printed in a form. The tabular format sacrifices some detail in favor of a readable printout. The print format can either use a print file width of at least 132, or forced into 79 columns by selecting the **Narrow print** option. The prints can be sorted differently than by key through the Sort differently checkbox.
Customize title	If this field is selected together with **Print format**, you can change the subtitle for the selection and add an extra title that is saved in your ISPF profile, your company name, department, and phone number for example. This flag setting is saved in your ISPF profile and is shared by all RA options showing it.
Send as email	If this field is selected along with **Print format**, then a panel opens for specifying the email address destination for the report. The email function does not work until you have configured the SMTP options with `SETUP OUTPUT`. This flag setting is saved in your ISPF profile and is shared between all RA options showing it.
Background run	If this field is selected together with **Print format**, then a batch job is submitted to perform the query. This flag setting is saved in your ISPF profile and is shared by all `RA` options showing it.
Full page form	If this field is selected (with a /) as well as **Print format**, then at least a full page per Digital Certificate is printed for including all certificate details. This selection is only effective when selected together with the **Print format** option. This flag setting is saved in your ISPF profile.

Table 152. Digital Certificate reporting - output and run options (continued)

Option	Description
Sort differently	If this field is selected together with **Print format**, then an alternate sort order can be selected. You can change the sort order in an ISPF display panel by issuing the SORT primary command in the ISPF panel. display. This flag setting is saved in your ISPF profile.
Narrow print	If this field is selected together with **Print format**, then the page width is limited to 79 characters, independent of the actual print file record length. If the field is not selected, then the page layout you specify must support a width of 132. However, the length can extend beyond that if the print file has a larger record length. This flag setting is saved in your ISPF profile and shared between all panels that support this option.

Digital certificates tabular display

A sample digital certificates display is shown in the following figure.

```
zSecure Suite  DIGTCERT CERTDATA segments          Line 1 of 5
Command ===> _____________________________________ Scroll===> CSR_
All certificates                                     29 Dec 2004 01:50
   Digital certificate labels       User     Tru Cert. sta Cert. end Complex
__ forConnectCERTAUTH               irrcerta Yes  5Sep2000  6Sep2001 PROD
__ forConnectSITE                   irrsitec Yes  5Sep2000  6Sep2001 PROD
__ l5 hightrust certificate         irrcerta Hi   6Sep2000  7Sep2001 PROD
__ typeDefault                      irrcerta Yes 10Jul2002 11Jul2003 PROD
__ x1                               irrsitec Yes  5Jul1999  6Jul2000 PROD
```

Figure 198. Digital certificates tabular display panel

The following fields of interest are shown.

Table 153. Digital certificates tabular display fields

Field	Description
Digital certificate labels	The certificate label of the certificate
User	The user ID associated with the certificate
Tru	Indicates whether the certificate is marked as trusted
Cert. sta	The date signifying the start of the validity of this digital certificate
Cert. end	The date signifying the end of the validity of this digital certificate
Complex	The security complex that contains the system. This can come from the ALLOC COMPLEX parameter or default to a system name.

By scrolling to the right, additional fields are displayed:

Field	Description
Issuer's distinguished name	The distinguished name of the issuer of the certificate.
Serial number	The serial number of the certificate.
Key Type	The type of the private key, stored in this digital certificate.

Field	Description
Subject's distinguished name	The distinguished name of the subject of the certificate, for example, the user for whom the certificate was issued.

Digital certificates detail display

Select any row on the digital certificate table display to see the detail view. Selection can be done by putting the cursor on the first character of row selection field and pressing ENTER, or by explicitly typing **S** there and pressing **Enter**.

```
zSecure Suite  DIGTCERT CERTDATA segments                    Line 1 of 32
Command ===> ____________________________________________ Scroll===> CSR_
All certificates                          29 Dec 2004 01:50
  Digital certificate labels
  forConnectSITE
  User     Tru
_ irrsitec Yes
  Subject's distinguished name
  CN=forConnectSITE
  Issuer's distinguished name
  CN=forConnectSITE
  Serial number
  00

_ CERTDATA segment                                              PROD
  Certificate startdate          5Sep2000  22:59
  Certificate enddate            6Sep2001  22:59
  Private Key Type              non-ICSF
  Private Key Size              0000
  Certificate lser              0000

  subjectAltName extension
  Certificate AltName email
  Certificate AltName domain
  Certificate AltName IP addr
  Certificate AltName URI

  keyUsage extension
  RACF format                   CERTSIGN
  X509 format                   keyCertSign cRLSign

  Ringname
_ CERT005.ringforConnectSITE
****************************** BOTTOM OF DATA ********************************
```

Figure 199. Digital certificates detail display panel

The following fields of interest can be shown:

Table 154. Digital certificates detail display fields

Field	Description
Digital certificate labels	The certificate label of the certificate
User	The user ID associated with the certificate
Tru	Indicates whether the certificate is marked as trusted
Certificate startdate	The date signifying the start of the validity of this digital certificate
Certificate enddate	The date signifying the end of the validity of this digital certificate
Subject's distinguished name	The distinguished name of the subject of the certificate, which represents the user for whom the certificate was issued.

Table 154. Digital certificates detail display fields (continued)

Field	Description
Issuer's distinguished name	The distinguished name of the issuer of the certificate.
Serial number	The serial number of the certificate.
Private Key Type	The type of the private key, stored in this digital certificate.
Private Key Size	The size, in bits, of the private key, stored in this digital certificate.
Certificate lser	It contains the last eight bytes of the last certificate that was signed with this key.
Certificate AltName email	The email addresses of the subject as found in the `subjectAltName` extension of the certificate.
Certificate AltName domain	The domain names of the subject as found in the `subjectAltName` extension of the certificate.
Certificate AltName IP addr	The IP addresses of the subject as found in the `subjectAltName` extension of the certificate.
Certificate AltName URI	The universal resource identifiers of the subject as found in the `subjectAltName` extension of the certificate.
RACF format	The `keyUsage` extension of the certificate as RACF would show it.
X509 format	The `keyUsage` extension of the certificate as defined by the X.509 standard.
Ring name	A list of full names (`userid` and `keyringname`) of the key rings to which this digital certificate is connected.

RA.C CUSTOM - User Defined Display (Custom Display)

In some situations, the standard display panels might not include fields you are interested in or the display might have the wrong selection or sort criteria. To resolve this problem, Security zSecure provides a method for testing `SELECT` and `DISPLAY` commands.

You can enter up to three `SELECT` commands. Any profile that matches the selection criteria is shown. The selections are combined with `OR` logic. Additionally, you can enter up to three `EXCLUDE` commands. A profile is shown as long as it does not match any of the exclusion criteria. The exclusion criteria are combined with `AND` logic. You can specify the `DISPLAY` command with any field name defined in the templates to select and show those records. Use the `TEMPLATE` primary command to look at the templates. For more information see “TEMPLATE - Template field properties” on page 284. You can also use the variables defined in the C2RXDEF1 member of the `SCKRCARL` library. The fields and variables are also documented in “RACF: RACF profiles” on page 1124.

For ease of use, the User Defined Display panel offers a suggested list of field names for each of the common profile classes. This list is added to the `DISPLAY` field when you type an *S* or `/` before the specific class name. Selecting a different common profile class does not overwrite what you typed in the `SELECT` or `EXCLUDE` fields.

Figure 200 on page 250 shows how some relevant fields are supplied for General Resource profiles.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - User defined display
Command ===> ____________________________________________________________

Enter up to 3 SELECT condition sets:
Select  ____________________________________________________________________
Select  ____________________________________________________________________
Select  ____________________________________________________________________
Enter up to 3 EXCLUDE condition sets:
Exclude ____________________________________________________________________
Exclude ____________________________________________________________________
Exclude ____________________________________________________________________
Enter output variables:
Display class(key)_key(44,key)_proftype(1)_uacc_owner_auditlvl_warning(1)_____
        complex_notify_seclabel_creadate_instdata_acl_acl:pgmrname_____________
        acl:instdata_/_appldata(header,"Application Data",20,detail)___________
        ____________________________________________________________________
        ____________________________________________________________________

Select a set of standard report variables for one of these profile classes:
 _  User    _  Dataset  _  Connect  s  General resource with cond.acc.list
 _  Group   _  Tape                _  General resource with member list
```

Figure 200. User-defined display panel

You can put together conditions and fields to fit your requirements of the day. For example, you might want to list all users who have requested a user ID but never used it.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - User Defined Display
Command ===> ____________________________________________________________

Enter up to 3 SELECT condition sets:
Select  c=user_ljtime=FFFFFFFF'x_creadate<dumpdate-14___________________________
Select  ____________________________________________________________________
Select  ____________________________________________________________________
Enter up to 3 EXCLUDE condition sets:
Exclude ____________________________________________________________________
Exclude ____________________________________________________________________
Exclude ____________________________________________________________________
Enter output variables:
Display key(8),name,dfltgrp,owner,creadate______________________________________
        ____________________________________________________________________
        ____________________________________________________________________
        ____________________________________________________________________
        ____________________________________________________________________
Select a set of standard report variables for one of these profile classes:
_  User    _  Dataset  _  Connect  _  General resource with cond.acc.list
_  Group   _  Tape                _  General resource with member list
```

Figure 201. Custom display

You can use the PRT or PRTLIST command on the Command input line to make a hard copy of the report to the ISPF LIST data set. Use the ISPF primary command **LIST** to send the contents of this data set to the printer.

The example query in the preceding figure results in the following display.

```
zSecure Admin User Defined Display             3 s elapsed, 1.1 s CPU
Command input ===>                                        Scroll===> CSR
                                                  11 Sep 1992 16:47
    Profile  Name                 DfltGrp  Owner    CreateDate
__ CICDDD1  G.N.N. CARD          CICD     CICD      2 Oct 1989
__ CIFOFVB                       CIFO     CIFO     27 Mar 1988
__ CISVIOF  R. LION              CISV     CISV      3 Jul 1989
__ CISVWKN  DRS. V.I.J. KNIFE    CISV     CISV      3 Jul 1989
__ CIWBOZB  FACULTY              CIWB     CIWB      8 Nov 1990
__ CLSTSES                       CLST     CLST     27 Mar 1988
__ CLSTSIS                       CLST     CLST     27 Mar 1988
__ CLSTSSA                       CLST     CLST     27 Mar 1988
__ CLSTSSP                       CLST     CLST     27 Mar 1988
__ CLSTSSQ                       CLST     CLST     27 Mar 1988
__ CLSTSSR                       CLST     CLST     27 Mar 1988
__ CLSTSSX                       CLST     CLST     27 Mar 1988
__ CLSTSSY                       CLST     CLST     27 Mar 1988
__ CLSTSSZ                       CLST     CLST     27 Mar 1988
__ CLSTTKV                       CLST     CLST     27 Mar 1988
__ CMISMR1                       CMIS     CMIS      3 Aug 1988
__ CNCATRP                       CNCA     CNCA     31 Oct 1988
__ COMBBOU  BOUMA, M,            COMB     COMB     17 Dec 1991
__ DDBLUEU  BLUE, PROF DR        DDBL     DDBL     20 Dec 1991
__ DDFEOOO                       DDFE     SYS1      6 Apr 1989
__ DDIGAAA                       DDIG     DDIG     22 Mar 1989
__ DDTEBEH                       DDTE     DDTE     10 Jan 1990
__ DMESALK  DARTS, DR IR         DMES     DMES     22 May 1992
__ DMESBAS                       DMES     DMES      3 Jan 1990
__ DMESGRA                       DMES     DMES      3 Jan 1990
__ DMESPR0  HOLDING - PRAKTICUM, DMES     DMES     25 Feb 1992
__ DMESPR1  HOLDING - PRAKTICUM, DMES     DMES     25 Feb 1992
__ DMESPR2  HOLDING - PRAKTICUM, DMES     DMES     25 Feb 1992
__ DMESPR3  HOLDING - PRAKTICUM, DMES     DMES     25 Feb 1992
__ DMESTEV                       DMES     DMES      3 Jan 1990
__
```

Figure 202. Custom query output display

The fields you can use in a query are documented in "RACF: RACF profiles" on page 1124.

Predefined CARLa scripts

zSecure provides predefined CARLa (CARLa Auditing and Reporting Language) scripts for creating the sample reports available in the SCKRCARL library. These scripts create reports for product panels and for printing. For information about the naming conventions for CARLa scripts, see "Naming convention" on page 706.

For more information, see the following topics:

- "Interactive reports"
- "CARLa scripts for RECREATE and COPY functions" on page 252
- "Report layouts" on page 252
- "Batch CARLa scripts" on page 253

Interactive reports

Table 155 describes the CARLa scripts for creating reports that display in the zSecure product panels.

Table 155. CARLa scripts to create Interactive reports

Report	Meaning
CKRDNONR	Creates the REPORT NONREDUNDANT sample display. The **RA.3.3** option in zSecure does not use this script.

Table 155. CARLa scripts to create Interactive reports (continued)

Report	Meaning
CKRDPROF	Creates the REPORT PROFILES sample display. The **RA.3.1** option in zSecure does not use this script.
C2RDRAS	Creates the CDT and SETROPTS class info. The **RA.S** in zSecure uses this script.
C2RDRASD	Creates the CDT and SETROPTS class info from database. The **RA.S** in zSecure uses this script.

CARLa scripts for RECREATE and COPY functions

The zSecure interactive component uses these CARLa scripts for COPY and RECREATE functions. The CKRX* CARLa scripts use LIKELIST clauses to refer to preselection NEWLIST statements with NAME=RACFSEL. To run these scripts with your own selections, define a preselection NEWLIST with that name. See "Selecting based on previously specified criteria (LIKELIST)" on page 887.

The CKGX* CARLa scripts can be concatenated with the corresponding CKRX* scripts. CKGX* can refer to RACFSEL either directly or through a specific preselection NEWLIST statement in the CKRX* CARLa script, GROUPS for example. These scripts issue CKGRACF commands in addition to the RACF commands generated in the CKRX* members to complete profile recreation.

Table 156 describes the CKGX* and CKRX* CARLa scripts in the product.

Table 156. CARLa scripts to recreate and copy data and profiles

CARLa script	Function
CKGXRDS	Recreate CKGRACF and user data for DATASET profiles.
CKGXRGR	Recreates CKGRACF and user data for group profiles.
CKGXRRES	Recreates CKGRACF and user data for resource profiles.
CKGXRUS	Recreate CKGRACF data, user data, and TSO data for User profiles.
CKRXCDS	Copy DATASET profile.
CKRXCRE	Copy general resource profile.
CKRXRAC	Recreate access list entries.
CKRXRDS	Recreate a DATASET profile.
CKRXRGR	Recreate a group profile.
CKRXRRE	Recreate a general resource profile
CKRXRUS	Recreate user

Report layouts

The following members contain the original layouts for the REPORT command when used with the indicated parameters. They are automatically included if the REPORT command is encountered with that parameter, while no REPORT_*type* NEWLIST precedes it in the query. (For REDUNDANT and NONREDUNDANT *type* equals NONREDUNDANCY; for the other parameters *type* equals the parameter name itself).

Member	Definitions
CKRREDUN	REPORT REDUNDANT default layout

Member	Definitions
CKRRNOND	REPORT NONDEFAULT default layout
CKRRNONR	REPORT NONREDUNDANT default layout
CKRROUTG	REPORT OUTOFGROUP default layout
CKRRPROF	REPORT PROFILES default layout
CKRRSCOP	REPORT SCOPE default layout

Batch CARLa scripts

Table 157 describes the CARLa scripts for creating reports through batch processing.

Table 157. CARLa scripts for creating reports through batch processing

CARLa script	Function
CKGXLIST	List profiles that require a `CKGRACF` refresh.
CKGXREFR	Create `CKGRACF REFRESH` commands for all profiles that require them.
CKGXUSRW	Create `CKGRACF WIPE` commands for `CKGRACF` and user data for all applicable user profiles.
CKRVDSN	Check consistency and completeness of data set resource protection.
CKRVPROG	Check consistency and referential integrity of program protection.
CKRVPWHC	Create `CKGRACF` commands to convert hashed passwords to DES-encrypted passwords
CKRVRACF	Check RACF database consistency.
CKRVUNIX	Create RACF commands to populate the `UNIXMAP` class.
C2RL$UNL	Create RACF and ACF2 unload and report statistics.

Chapter 3. RACF Audit Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

General information

The interactive component of Security zSecure is an ISPF application available under MVS/TSO.

For details on how to start this component, see "Starting the interactive component" on page 9. See "Panel structure" on page 10 for an overview of the panels and instructions for using them.

After selecting the **AU Audit** option, the panel should look similar to the one shown in Figure 203.

```
  Menu         Options       Info     Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - Main menu
Option ===> ____________________________________________________________________
                                                                        More      +
SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
  C    Change track   Track changes to the system
  L    Libraries      Library status and update analysis
  S    Status         Status auditing of security and system tables/options
  V    Verify         Verify and cleanup security database
RE   Resource        Resource reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

 Input complex: Active backup RACF data base

Product/release:
5655-T01 IBM Security zSecure Admin 1.13.0
5655-T02 IBM Security zSecure Audit for RACF 1.13.0
```

Figure 203. IBM Security zSecure Admin main menu

This section of the documentation focuses on Audit functions. For more information on the Audit menu options, refer to the sections indicated in Table 5-1 the following table. For a table of references for the other main menu options such as RA and EV , see Table 2 on page 11. You can also obtain information about the panels and fields by using the context-sensitive help function available on most panels. To access the help, press PF1 or type HELP.

The options in the Audit main menu are described in different manual sections.

Table 158. Documentation reference for zSecure Menu options

Menu Option	Documentation reference
SE Setup	"SE SETUP - Options and input data sets used" on page 1641

Table 158. Documentation reference for zSecure Menu options (continued)

Menu Option	Documentation reference
RA RACF	Chapter 2, "RACF Administration Guide," on page 51
AU.C	"AU.C Change track" on page 521
AU.L	Chapter 6, "Library Audit Guide," on page 529
AU.S	Information about the part of the AU.S menu option that pertains to an MVS system is provided in "STATUS AUDIT - MVS tables" on page 440 and "STATUS AUDIT - MVS extended tables" on page 499.
AU.V	"AU.V VERIFY - Verify Selection List" on page 353

This Audit Guide includes the following sections:

"Migrating from DSMON": Migration from DSMON.

"AU.S STATUS AUDIT - MVS and RACF security options and tables" on page 257: A description of the STATUS AUDIT menu.

"STATUS AUDIT - OVERVIEW" on page 261: Overall audit concern overview ordered by audit priority.

"STATUS AUDIT - RACF control" on page 266: A discussion of the RACF audit reports.

"STATUS AUDIT - RACF user" on page 291: A description of RACF reports on RACF user IDs.

"STATUS AUDIT - RACF resource" on page 316: A description of RACF reports on the protection of resources, resource profile audit concerns, and database resource usage.

"AU.V VERIFY - Verify Selection List" on page 353: Reports on inconsistencies, and how to solve these.

"Common RACF problems" on page 356: Solutions to some of the most common problems.

"Auditing CKGRACF" on page 371: A discussion on auditing the CKGRACF authorized component.

"Predefined CARLa scripts" on page 377: A discussion of the sample reports available, and their use.

Migrating from DSMON

The DSMON (Data Security Monitor) program is part of the RACF security system. Many auditors use this program for audit reporting and analysis. You can use zSecure to create the equivalent DSMON reports. In addition, zSecure provides many additional reports that provide more detailed and extensive audit reporting.

Use the information in this chapter to learn how to create the equivalent DSMON reports using zSecure. For information about the DSMON program, see the *Security Server RACF Auditor's Guide*.

For information about the reports, see the following topics:

- DSMON System Report See "SYSTEM - MVS system settings report" on page 441.
- DSMON Group Tree Report See "RA.3.8 GROUP TREE - Group tree display" on page 217.
- DSMON Program Property Table Report See "PPT - Program Property Table report" on page 467.
- DSMON Authorized Caller Table Report See "AUTAB - RACF Authorized Caller Table ICHAUTAB" on page 273.
- DSMON Class Descriptor Table report See "RACFCLAS - Class Descriptor Table report" on page 277.
- DSMON Exits Report See "EXITS - Exit and table report" on page 501
- DSMON Global Access Checking report See "GLOBAL - Global Profile overview" on page 283.
- DSMON Started Procedure Table Report See "STCTABLE - Started Procedure Table and Started Class" on page 288, "STCPROT - Started Task protection report" on page 344, and the VERIFY STC command.
- DSMON User Attribute Report See "AUTHSYS - System Authorization reports" on page 297 and "AUTHGRP - Group Authorization report" on page 299.
- DSMON Data Set Reports See "SENSITIVE - Sensitive Data Set report" on page 518, "SENSPROF - Sensitive Data by Profile report" on page 321, "SENSTRUS - Sensitive Data Trustees report" on page 317, and the VERIFY SENSITIVE command.

AU.S STATUS AUDIT - MVS and RACF security options and tables

The AU.S Audit Status option shows the contents of MVS and RACF security tables and settings. The first menu is displayed in Figure 204.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Audit - Audit - Status
Command ===> ____________________________________________________________

Enter / to select report categories
_ MVS tables      MVS oriented tables (reads first part of CKFREEZE)
_ MVS extended    MVS oriented tables (reads whole CKFREEZE)
_ RACF control    RACF oriented tables
_ RACF user       User oriented RACF tables and reports
_ RACF resource   Resource oriented RACF tables and reports

 Select options for reports:                                  Audit policy
 _   Select specific reports from selected categories         /  zSecure
 /   Include audit concern overview in overall prio order     _  C1
 _   Only show reports that may contain audit concerns        _  C2
 __   Minimum audit priority for audit concerns (1-99)       _  B1
 _   Print format             _  Concise (short) report
```

Figure 204. STATUS AUDIT menu

The available reports are divided into a number of categories.

- **MVS TABLES** and **MVS EXTENDED** provide audit reports for MVS security tables and settings. For information, see "STATUS AUDIT - MVS tables" on page 440. You can create these reports using zSecure Audit for RACF.
- **RACF CONTROL** provides reports on the global system protection, classes, and database template. These reports do not require a full CKFREEZE read.
- **RACF USER** provides general and detail reports on the RACF users. Typically, these reports generate a **lot** of output. The `TRUSTED` report requires a full `CKFREEZE` read.
- **RACF RESOURCE** provide reports on resource protection for resources like data sets and UNIX files, resource profile audit concerns, and database resource use.

Type a / in the selection field for a report category to open the report selection panels to set up and create the reports.

You can specify the following processing parameters on the report selection panel:

Select specific reports from selected categories
If you select this option, a follow-up report selection panel opens for each selected category. If you do not select this option, all reports in the selected categories are generated.

Include audit concern overview in overall prio order.
This option determines whether an audit concern overview is generated. This overview shows up as the first item in the output. It is sorted by audit priority, and contains a single line for each item for which audit concerns were identified, including an indication of which report the item occurs in. Note that not all reports explicitly identify audit concerns; they are not represented here. The overview spans the categories selected (not just the selected reports). If you select this option without selecting any categories, an overview for all categories is generated. If you only want an overview across a specific category, you can select that category along with the *Select specific reports from selected categories* option, but not select any of the reports.

Only show reports that may contain audit concerns
If you select this option, only the reports that can contain audit concerns are displayed. If *Select specific reports from selected categories* is also requested, only the reports that can contain audit concerns are selectable.

Minimum audit priority for audit concerns (1-99)
Specify the minimum audit priority for audit concerns or leave blank for all records.

Print format
For a foreground run, selecting this option requests to present the output in a printable report format instead of as interactive displays. This is preferable if memory is tight or the output is to be printed. For a detail study of a small amount of data, the interactive display format is generally better suited. For a background run, this option has no effect.

Concise (short) report
If you select this option, some details are omitted from the generated reports. If you are looking for changes or if you are exploring the system, we advise you to select this option; if you want to audit a particular item in depth, you should not use it.

Background run
If you select this option, a background (batch) job is submitted for the

requested reports,which implies output in print format. If you do not select this option, processing proceeds in the foreground.

Audit policy
Use this option to select the audit policy for etermining the audit concerns and priorities. The default audit policy raises the priority value of an audit concern to 40 or more if the system can almost certainly be compromised as a result of the concern. The *C1*, *C2*, and *B1* selections refer to the DoD orange book standards. These values also raise the priority value to 40 or more when a violation of the selected policy is discovered. Specifying these selections does not imply that all violations are noted. In addition, *B1* generates more audit concerns.

If foreground processing is selected, Security zSecure displays the number of `CKFREEZE` records read during processing. After processing, the resulting output is displayed. You can stop report processing by pressing the **ATTN** key.

If background processing is selected, a submit panel is displayed for browsing or editing the generated JCL, and then submit a batch job.

Some reports have additional selection options available to customize the reports. When you select these reports, the panels for these customization options open in sequence so you can specify the settings. You can learn more about the report options available in the report descriptions provided in this manual. When you first use the product, you can leave the selection options blank to use the default values for creating the report. Then, you can study the basic report to determine whether you need to customize the report.

If you select a set of system reports without specifying the disposition options, Security zSecure creates a report selection list with the report types selected as shown in Figure 205 on page 260. The report type list varies depending on what report types you selected from the STATUS - Audit panel (Figure 204 on page 257).

```
zSecure Audit Display Selection                    Line 1 of 84
 Command ===> _____________________________________________ Scroll===> CSR

  Name     Summary Records Title
_ OVERVIEW    7686       0 Audit concern overview by priority (higher prioritie
_ SETROPTS       2       2 RACF system, ICHSECOP, and general SETROPTS settings
_ SETROPAU       2      12 SETROPTS settings - audit concerns
_ ROUTER         2     372 ROUTER - SAF router table (ICHRFR01)
_ AUTAB          0       0 RACF Authorized Caller Table
_ RANGE          2       2 RACF Range Table
_ RACFDSN        2       4 RACF Current database data set names and settings
_ RACFCLAS       2     329 RACF CDT, SETROPTS class info and number of profiles
_ GLOBAL         2      10 Global profile overview
_ TEMPLATE       1     739 RACF template definitions
_ STARTED        1     134 RACF Profiles in Started Class - sorted by procedure
_ STCTABLE       1     108 RACF Started Procedure Table - sorted by procedure
_ TRUSTUSR       1    6040 Trusted userids (may bypass security)
_ AUTHSYS        2      44 Users with system-wide special, operations, auditor,
_ AUTHUID0       1      13 Users with uid 0
_ AUTHGRP        2     161 Users with group level special, operations, auditor
_ SHRDUIDS       1      97 OMVS UIDs shared between RACF users
_ OMVSNUID       1       9 RACF users with OMVS segment but no UID
_ SHRDGIDS       1      25 OMVS GIDs shared between RACF groups
_ OMVSNGID       1       9 RACF groups with OMVS segment but no GID
_ PROTECT        1      40 Protected users
_ PWNONE         0       0 Users who can logon without password
_ PWOID          0       0 Users who can logon with OIDcard
_ PWINNONE       2     190 Users without password interval
_ PWINLONG       2     467 Users with password interval > 60 days
_ PWEXPIRE       2    2419 Users with expired passwords
_ PWNOCHG        2    1293 Users that never changed password
_ PWAGESUM       2    2582 RACF password age overview
_ PWAGEALL       2    2582 User Password Age: All users
_ PWAGENEV       2    1293 User Password Age: Initial password
_ PWAGE5YR       2    1141 User Password Age: 5 years or more
_ PWAGE4YR       1      15 User Password Age: 4..5 years
_ PWAGE3YR       1      17 User Password Age: 3..4 years
_ PWAGE2YR       1      25 User Password Age: 2..3 years
_ PWAGE1YR       1      26 User Password Age: 1..2 years
_ PWAGE0YR       1      65 User Password Age: Less than a year
_ PWAGE6MN       1      24 User Password Age: 6..12 months
_ PWAGE5MN       1       6 User Password Age: 5..6 months
_ PWAGE4MN       1       2 User Password Age: 4..5 months
_ PWAGE3MN       1       2 User Password Age: 3..4 months
_ PWAGE2MN       1       2 User Password Age: 2..3 months
_ PWAGE1MN       1      14 User Password Age: 1..2 months
_ PWAGE2WK       1       2 User Password Age: 2..4 weeks
_ PWAGEREC       1      13 User Password Age: Less than 2 weeks
_ PWTRIES        2     126 Users with logon failures
_ LGNEVER        2     693 Users that have never been used
_ LGNOREV        1       1 Systems that do not revoke users due to inactivity
_ LGREVOKE       1      76 Users pending revoke because of inactivity
_ LGAGESUM       2    2622 RACF last logon overview
_ LGAGEALL       2    2622 User Last Logon: All users
_ LGAGENEV       2    1039 User Last Logon: Never logged on
_ LGAGE5YR       2    1433 User Last Logon: 5 years or more ago
_ LGAGE4YR       1      15 User Last Logon: 4..5 years ago
_ LGAGE3YR       1      19 User Last Logon: 3..4 years ago
_ LGAGE2YR       1      13 User Last Logon: 2..3 years ago
_ LGAGE1YR       1      16 User Last Logon: 1..2 years ago
_ LGAGE0YR       1      87 User Last Logon: Less than a year
_ LGAGE6MN       1      27 User Last Logon: 6..12 months ago
_ LGAGE5MN       1       3 User Last Logon: 5..6 months ago
_ LGAGE4MN       1       7 User Last Logon: 4..5 months ago
_ LGAGE3MN       1       1 User Last Logon: 3..4 months ago
_ LGAGE2MN       1       6 User Last Logon: 2..3 months ago
_ LGAGE1MN       1       4 User Last Logon: 1..2 months ago
_ LGAGE2WK       1       3 User Last Logon: 2..4 weeks ago
_ LGAGEREC       1      36 User Last Logon: Less than 2 weeks
_ RACPRAUD       2     931 RACF profile audit concerns
_ SENSTRUS       2    6040 Sensitive data trustees
_ SENSPROF       1     153 Profiles covering sensitive data sets
_ ENTITY#S       2   10800 Entity segment summary by descending number of bytes
_ SEGMENT        2   10800 Class segment summary by descending number of bytes
 _ TSOAUTH       1     136 TSO authorized commands
_ LPAPROT        1     543 LPA module protection overview
_ APFPROT        1    1542 APF module protection overview (except UNIX files)
_ UNIXAPF        1      83 UNIX files with APF authorization
_ UNIXCTL        1     665 UNIX files that are program controlled (daemons etc)
_ UNIXSUID       1     106 UNIX files with SETUID authorization
_ UNIXSGID       1      13 UNIX files with SETGID authorization
_ PADS           0       0 PADS module protection overview
_ STCPROT        2    1841 Started task overview
_ GLBWDSN        1      32 Data sets vulnerable to trojan horse & back door att
_ GLBWUNIX       1      57 UNIX files vulnerable to trojan horse & back door at
_ UIDNOUSR       1   55746 UIDs not defined in the complex
_ GIDNOGRP       1   55746 GIDs not defined in the complex
******************************* Bottom of data ********************************
```

Figure 205. RACF Security report selection display

The reports in Figure 205 on page 260 provide information about RACF security tables and settings. For more information, see “STATUS AUDIT - MVS tables” on page 440.

For information about MVS security tables and settings, see “STATUS AUDIT - MVS extended tables” on page 499.

zSecure assigns a numerical *audit priority* to each system report entry, indicating the need to review the entry.

- Higher numbers indicate greater concern.
- Numbers 20 and up require review.
- Numbers 40 and up require immediate attention.

Each report entry with a high audit priority also has an associated *audit concern* in text-format. The audit concern summarizes the problem that requires review.

The RACF report types generally have the following structure:

- Summary information sorted by system
- An overview panel,
- A detail panel

Typically, the overview panels are sorted by descending audit priority. That is, the most important entries are listed first. In an overview display, you can view the most important audit concerns by scrolling to the right. In a detail display, you can view all audit concerns by scrolling max down.

STATUS AUDIT - OVERVIEW

The OVERVIEW report at the top of the selection list is a good point to start a system audit. The report summarizes the most important audit concerns across all report types and all systems audited, sorted by numerical audit priority. A pointer to the relevant report type is included. We suggest you view this report first, and then explore the other reports, starting with the reports having the highest audit priority. Figure 206 shows an audit overview display.

```
Audit concern overview by priority (higher priorities only)     Line 1 of 3247
Command ===>                                                   Scroll===> CSR
                                          7 Sep 2000 00:07
   Pri Complex  Syst Area Key         Audit concern
s_  22 TODAY         FILE ...         .profile in user's home directory is worl
__  22 TODAY    DINO CLAS DEVICES     Devices like ESCON directors, FEPs, local
__  20 TODAY    DINO CLAS TEMPDSN     Temporary datasets resident after failure
__  20 TODAY    DINO SETR OPERAUDIT N OPERATIONS activity undetectable
__  11 TODAY         FILE checkpass   executable file runs APF-authorized (exta
__  11 TODAY         FILE ...         file is world writable
__  11 TODAY         FILE ...         directory is world writable
__  11 TODAY    DINO SETR RVARYSTAT N Password to deactivate RACF still at IBM
__  10 TODAY         FILE .../util.c  file is world writable
__  10 TODAY         RACF &CRMNODE.RU Verify why UACC>=UPDATE
__  10 TODAY         SENP C##A.X.**   No update audit
__  10 TODAY         SENP C##B.T.**   No alter audit
```

Figure 206. RACF Security audit overview display

The overview report contains the following fields of interest:

Field	Explanation
Pri	Numerical audit priority, identifying the severity of the problem. Priorities of 40 and up indicate a very serious concern, requiring immediate attention. Priorities in the range 20 to 39 require review because serious security threats might exist.
Complex	The name of the complex including the system on which the audit concern was identified.
Syst	The name of the system on which the audit concern was identified.
Area	The report type in which the audit concern was identified.
Key	The report key identifying the entry within the relevant report. The value and meaning of the key is report dependent.
Audit concern	The audit concern identified. Background information and audit considerations are explained with each report type.

The following table lists the abbreviations and the NEWLIST types for the various report types. The page numbers refer to the audit concern sections.

Table 159. NEWLIST types - associated report abbreviations and types

Abbreviation	Report type	NEWLIST type
CLAS	Class Descriptor Table	CLASS (page 990)
CONS	Console	CONSOLE (page 1004)
DASD	DASD volume	DASDVOL (page 1013)
DMS	SAMS:Disk parameters	AUDIT (page 961)
EXIT	Exit	EXIT (page 1029)
FILE	UNIX files	UNIX (page 1481)
HSM	Hierarchical Storage Manager	AUDIT (page 961)
IOAP	I/O appendage	IOAPP (page 1052)
JCL	JES2 job class	JOBCLASS (page 1090)
MOUN	Unix Mount Points	MOUNT (page 1104)
MSG	Message Processing Facility	MSG (page 1107)
MVS	MVS Properties	AUDIT (page 961)
PPT	Program Property Table	PPT (page 1122)
RACF	RACF profiles	RACF (page 1131)
SENP	Sensitive profiles	REPORT_SENSITIVE (page 1242)
SENS	Sensitive data sets	SENSDSN (page 1256)
SETR	SETROPTS settings	AUDIT (page 961)
SMF	SMF system settings	AUDIT (page 961)
SMFO	SMF subsystem	SMFOPT (page 1403)
SSCT	Subsystem	SUBSYS (page 1407)
STOR	Writable common storage	CSM (page 1009)
SVC	SuperVisor Call	SVC (page 1417)
SYSL	Syslog settings	AUDIT (page 961)
TRUS	Trusted users and sensitive resources	TRUSTED (page 1476)

Table 159. NEWLIST types - associated report abbreviations and types (continued)

Abbreviation	Report type	NEWLIST type
TSO	TSO settings	AUDIT (page 961)
VSM	Virtual Storage Map	VSM (page 1493)

If you select one of the audit concerns listed with the **S** action character, a detail display is shown.

```
Audit concern overview by priority (higher priorities only)       Line 1 of 22
Command ===>                                                    Scroll===> CSR

                                                 7 Sep 2000 00:07

System
Complex name                    TODAY
System name                     DINO

Audit concern
Relative audit priority         22
Audit concern                   .profile in user's home directory is world
Audit concern                   writable

UNIX file
Absolute pathname               /u/c##qa100/.profile
FS mounted with SECURITY        Yes
FS mounted with SETUID          Yes
FS mounted READ/WRITE           Yes
File type                       -
File access attributes          a=w
Extended file attributes        +s -ap
User id                         80000100
Owner name                      C##QA100
Group id                        0
Group name                      Zsecur C##A SYSAPPL SYSPROG SYS1
******************************** BOTTOM OF DATA ********************************
```

The detail display layout depends on the report type in which the audit concern was identified; the preceding example shows the layout for a FILE concern. For FILE you usually need to look at the detail display to see what UNIX file it really applies to, since the 11 positions for **Key** on the overview tend to show '...' (meaning that the relative path name really did not fit at all) or '*.../lastqual*'. This example shows that all have write access to file /u/c##qa100/.profile (a=w), while this is a .profile file in some user's home directory, which means it can be executed when that user logs on.

The detail display repeats the following report-independent fields of interest (in full):

Field	Explanation
Complex name	The complex name
System name	The system name
Relative audit priority	The severity of the concern
Audit concern	The audit concern identified

Note: The SENP details omit the system information, as it is not applicable. The TRUS details do not report Complex and System as identification at the top (as multiple systems can be involved).

The detail display also contains a report-dependent section, containing the fields mentioned in the following tables. See “STATUS AUDIT - MVS tables” on page 440 and “STATUS AUDIT - MVS extended tables” on page 499 for information about the following types of data: `CONS`, `DASD`, `DMS`, `EXIT`, `HSM`, `IOAP`, `JCL`, `MOUN`, `MSG`, `MVS`, `PC`, `PPT`, `SENS`, `SMF`, `SMFO`, `SSCT`, `STOR`, `SVC`, `SYSL`, `TSO`, and `VSM` details.

Table 160. CLAS - RACF Class

Field	Explanation
Class name	The class name
Protection active	Whether the class is used for protection
Class description	An explanation of the purpose of the class

Table 161. FILE - UNIX files

Field	Explanation
Absolute pathname	The full pathname of the file.
FS mounted with SECURITY	Whether the file system is mounted with the SECURITY attribute. If not, any user can access and change any file in it.
FS mounted with SETUID	Whether the file system is mounted with the SETUID attribute. Setuid, setgid, APF, and program control attributes are only honored if so.
FS mounted READ/WRITE	Whether the FS is mounted read/write (Yes) or read-only (No).
File type	The type of file: regular file (-), block special file (b), character special file (c), directory (d), external symlink (e), symlink (l), pipe or FIFO (p), socket (s).
File access attributes	The effective file mode, shown as lists of permissions for specific groups. The groups are owner (u), group (g), and other (o). When the permissions of all groups are equal, an (a) is used. The permissions can be read (r), write (w), execute (x), setuid/setgid (s), and sticky bit (t). The setuid/setgid and sticky bits indicators are shown in uppercase (S/T) when execute permission is off. Note that this format is the same as used by the chmod command. These are effective permissions meaning that the mount attributes NOSECURITY and NOSUID as well as the mount MODE (read/write or read-only), and the directories in the file's path have been taken into account.
Extended file attributes	The effective extended attributes, shown as a list of attributes that are on (+) and a list of attributes that are off (-). Possible attributes are APF authorization (a), program controlled (p), address space sharing (s), and library sharing (l).
User id	The `uid` for the file owner.
Owner name	The RACF `userids` mapped to this uid.
Group id	The `gid` for the file.
Group name	The RACF group(s) mapped to this gid.

Table 162. RACF - RACF profiles

Field	Explanation
Class	The profile class.
Profile key	The profile key.

Table 162. RACF - RACF profiles (continued)

Field	Explanation
Universal access authority	The universal access level.

Table 163. SENP - Sensitive profiles

Field	Explanation
Profile type	The profile type.
Profile key	The profile key.
Universal access authority	The universal access level.
Audit access success/failures	The minimum access level for success auditing (if it occurs) and for failure auditing (if it occurs).
Erase-on-scratch	The erase-on-scratch setting for the profile (the SETROPTS setting and HSM settings must also be on for actual erasure on deletion).

Table 164. SETR - SETROPTS settings

Field	Explanation
Parameter name	The RACF parameter.
Parameter value	The value the parameter is set to.

Table 165. TRUS - Sensitive data trustees

Field	Explanation
Complex that may be attacked	The complex for the security database at risk.
System that may be attacked	The system at risk.
Type of sensitive resource	The type of sensitive resource: • *APF library* • *Resource*–a FACILITY profile granting a privilege for example • *Surrogate* – permitting work to be performed under another identity. • *TrustedHome*. The UNIX home directory of a trusted user. • *Privilege*. A privilege affecting the entire system.
Resource class	The resource class, which can be *System*for a system-wide privilege like SPECIAL.
Resource name	The resource name. This value can represent the name of a system for a system-wide privilege.
Volume serial for resource	Volume serial for the resource (if applicable).
Access level that is exposure	The minimum access level that is considered sensitive.
Complex used for the attack	The complex name for the security database where the trusted access is granted.
RACF profile class	The class of the profile which grants access, or an identifier which describes the domain of the privilege.
RACF profile	The security rule by which access is granted.

Table 165. TRUS - Sensitive data trustees (continued)

Field	Explanation
Trusted userid	The user granted trusted access.
Privilege on user's complex	The privilege, security attribute, or operating system function that grants the user access.
Id associated with privilege	The group ID that grants the user access (when access is given via a group.)
Access level granted to user	The access granted if applicable to the privilege.

STATUS AUDIT - RACF control

The RACF reports on global system protection, classes, and database templates do not require a full CKFREEZE read.

More RACF reports are available in the CARLa library or from the main menu options **RA** and **AU.V**. You are advised to run the collection batch report CKRL$ALL, which includes other reports, at least once.

The following RACF reports are described in this section:

- SETROPTS - RACF settings report
- SETROPTD - RACF SETROPTS settings in database
- RRSFNODE - RACF Remote Sharing Facility settings
- ROUTER - SAF router table (ICHRFR01)
- AUTAB - RACF Authorized Caller Table ICHAUTAB
- RANGE - RACF Range Table ICHRRNG
- RACFDSN - RACF Data Set Name Table ICHRDSNT
- RACFCLAS - Class Descriptor Table report
- RACFDCLS - RACF class info from database ICB
- GLOBAL - Global Profile overview
- TEMPLATE - Template field properties
- STCTABLE - Started Procedure Table and Started Class

SETROPTS - RACF settings report

STATUS AUDIT option SETROPTS shows the system-wide RACF options as shown by the SETROPTS command, combined with information from the ICHSECOP module and the CDT. A second report SETROPAU shows the associated audit concerns. These reports are only available on z/OS systems and require system information. You must supply an input set that has at least one of the following data sources: a CKFREEZE data set, Live system, or active RACF allocation.

These reports are only available on z/OS systems and require access to system information from one of the following input data sources: the CKFREEZE data set, live system, or active RACF allocation.

```
RACF system, ICHSECOP, and general SETROPTS settings              Line 1 of 67
Command ===> _____________________________________________ Scroll===> CSR_

                                                  23 Mar 2005 00:07
   Complex  System   Collect time stamp
   DINO     DINO     23 Mar 2005 00:07

General RACF properties                 Data set protection options
Access Control active          Yes      Prevent duplicate datasets    No
Force storage below 16M        No       Protectall                    Yes/fail
Check all connects  GRPLIST    Yes_____ Automatic Dataset Protect     No______
Check genericowner for create  Yes_____ Enhanced Generic Naming       Yes_____
NOADDCREATOR is active         Yes_____ Prefix one-level dsns         ONEQUAL_
Dynamic CDT active             No       Prevent uncataloged dsns      No______
RACF local node                DINO     GDG modelling                 No______
RRSF propagate RACF commands   No       USER modelling                No______
RRSF propagate applications    No       GROUP modelling               No______
RRSF propagate passwords       No
RRSF honour RACLINK PWSYNC     Yes
Application ID mapping stage   0
Level of KERB processing       __0
Primary Language               ENU
Secondary Language             ENU
RACF software release level    HRF7707 OA03853
RACF DB template level         OA03853

DASD data set protection                Terminal protection
Volume level permits DASDVOL   No       Terminal protection active    Yes
Erase-on-scratch               All      Undefined terminal TERMUACC   NONE____

TAPE data set protection                Program protection
Tape dataset check TAPEDSN     No______ Program control WHEN(PROGRAM) Yes_____
Tape volume protection active  Yes      Program control mode          Basic
Protection duration RETPD      00000___

Auditing options                        Mandatory Access Control options
Audit SPECIAL users            Yes_____ Require SECLABEL     MLACTIVE No______
Audit OPERATIONS users         Yes_____ Prevent declassify   MLS      No______
Audit USER profile changes     Yes_____ Stabilize labels     MLSTABLE No______
Audit GROUP profile changes    Yes_____ Label maintenance    MLQUIET  No______
Audit SECLABELed resources     No______ No SECLABEL tolerate COMPAT   No______
Audit command violations       Yes_____ Special required SECL.CONTROL No______
Audit from security level      None     Req. labels UNIX fs  MLFSOBJ
Real datasetnames in SMF       No______ Req. labels IPC obj  MLIPCOBJ
Dataset logoptions             Profile  Name hiding active   MLNAMES
APPLAUDIT is active            No______ Labels by system SECLBYSYSTEM

Identification/Authentication options   Job Entry Subsystem options
Remember dates INITSTATS       Yes_____ Batch userid req BATCHALLRACF Yes_____
Prevent logon if unused days   255_____ Monitor userid req XBMALLRACF No _____
Revoke after password attempt  __5_____ Call router exit  EARLYVERIFY No _____
Old passwords forbidden        _32      Default uid remote  NJEUSERID ????????
Password change wait days      _No      Default uid local  UNDEFINEDU ++++++++
Password change interval       _90_____
Password change warning day    _10_____
Mixed case passwords allowed   No______
Key change required day        None____
RVARY SWITCH password set      No
RVARY STATUS password set      No

Password rules
Password rule 1
Password rule 2                LLLLL*** LENGTH(5:8)
Password rule 3
Password rule 4
Password rule 5                L*C*CN** LENGTH(6:8)
Password rule 6
Password rule 7
Password rule 8
Legend: $-national  A-alpha   c-mixed cons. C-consonant L-alphanum
        m-mixed num N-numeric v-mixed vowel V-vowel     W-novowel  *-anything

EIM registry
NONE
****************************** Bottom of Data ******************************
```

The RACF settings audit concerns report SETROPAU shows the audit concerns identified.

The following figure shows a sample RACF audit concerns summary display.

```
SETROPTS settings - audit concerns                                Line 1 of 4
Command ===>                                                   Scroll===> CSR
                                                    7 Sep 2000 00:07
   Pri Complex  System   Count
    20 TODAY    DINO         4
   Pri Parameter                Value    Audit concern
s_  20 OPERAUDIT                No       OPERATIONS activity undetectable
__  11 RVARYSTATUSPWSET         No       Password to deactivate RACF still at I
__  10 RVARYSWITCHPWSET         No       Password to switch RACF database still
__   2 TAPEDSN                  No       Tape datasets are unprotected unless T
****************************** BOTTOM OF DATA *********************************
```

The display contains the following fields of interest.

Field	Explanation
Pri	The highest priority for any audit concern for this system.
Complex	The complex name for the security database.
System	The system name.
Count	The number of audit concerns for this system.
Pri	A measure for the severity of the audit concern.
Parameter	The RACF setting that causes the audit concern
Value	The parameter's value.
Audit concern	The audit concern identified for this setting.

Select an audit concern for a detail display.

```
SETROPTS settings - audit concerns                                Line 1 of 12
Command ===>                                                   Scroll===> CSR
                                                    7 Sep 2000 00:07
System
Complex name                TODAY
System name                 DINO
SETROPTS setting
Parameter name              OPERAUDIT
Parameter value             No
Audit concern
Relative audit priority     20
Audit concern               OPERATIONS activity undetectable
****************************** BOTTOM OF DATA *********************************
```

The detail display shows no additional information.

SETROPTD - RACF SETROPTS settings in database

STATUS AUDIT option SETROPTD shows the RACF SETROPTS settings as found in the RACF database or an unloaded database. A second report SETROPAD shows the associated audit concerns.

```
SETROPTS settings in database                                  Line 1 of 55
Command ===> _____________________________________________ Scroll===> CSR_
                                          22 Aug 2003 00:07
   Complex
   DINO

Dataset protection options          General RACF properties
Protectall                 Yes/fail RACF Resource Access Ctl Fac  2.6.0
Automatic Dataset Protect  No______ Level of KERB processing
Enhanced Generic Naming    Yes_____ Check all connects  GRPLIST   Yes_____
Prefix one-level dsns      ONEQUAL_ Check genericowner for create Yes_____
Prevent uncataloged dsns   No______ NOADDCREATOR is active        Yes_____
GDG modelling              No______ Application ID mapping stage
USER modelling             No______ Primary Language              ENU
GROUP modelling            No______ Secondary Language            ENU

DASD dataset protection             Terminal protection
Volume level permits DASDVOL  No    Terminal protection active    No
Erase-on-scratch              All   Undefined terminal TERMUACC   READ____

TAPE dataset protection             Program protection
Tape dataset check TAPEDSN    No____ Program control WHEN(PROGRAM) Yes_____
Tape volume protection active Yes
Protection duration RETPD     00000___

Auditing options                    Mandatory Access Control options
Audit SPECIAL users        Yes_____ Require SECLABEL     MLACTIVE No______
Audit OPERATIONS users     Yes_____ Prevent declassify   MLS      No______
Audit USER profile changes Yes_____ Stabilize labels     MLSTABLE No______
Audit GROUP profile changes Yes____ Label maintenance    MLQUIET  No______
Audit SECLABELed resources No______ No SECLABEL tolerate COMPAT   No______
Audit command violations   Yes_____ Special required SECL.CONTROL No______
Audit from security level  None     Req. labels UNIX fs  MLFSOBJ
Real datasetnames in SMF   No______ Req. labels IPC obj  MLIPCOBJ
Dataset logoptions         Profile_ Name hiding active   MLNAMES
APPLAUDIT is active        No______ Labels by system SECLBYSYSTEM

Identification/Authentication options  Job Entry Subsystem options
Remember dates INITSTATS   Yes_____ Batch userid req BATCHALLRACF Yes_____
Prevent logon if unused days 255____ Monitor userid req XBMALLRACF No______
Revoke after password attempt __5___ Call router exit  EARLYVERIFY No______
Old passwords forbidden    _32      Default uid remote  NJEUSERID ????????
Password change wait days  _No      Default uid local  UNDEFINEDU ++++++++
Password change interval   _90_____
Password change warning day _10_____
Mixed case passwords allowed No_____
Key change required day    None____
RVARY SWITCH password set  No
RVARY STATUS password set  No

Password rules
Password rule 1
Password rule 2            LLLLL*** LENGTH(5:8)
Password rule 3
Password rule 4
Password rule 5            L*C*CN** LENGTH(6:8)
Password rule 6
Password rule 7
Password rule 8
Legend: $-national  A-alpha   c-mixed cons. C-consonant L-alphanum
        m-mixed num N-numeric v-mixed vowel V-vowel     W-novowel  *-anything
****************************** BOTTOM OF DATA ********************************
```

The RACF settings audit concerns report SETROPAD shows the audit concerns identified.

The following figure shows a sample RACF audit concerns summary display.

```
SETROPTS settings - audit concerns                              Line 1 of 4
Command ===>                                                 Scroll===> CSR

                                          30 Aug 2002 10:01
   Pri Complex  System   Count
    20 TODAY    DINO         4
   Pri Parameter               Value    Audit concern
s_  20 OPERAUDIT               No       OPERATIONS activity undetectable
__  11 RVARYSTATUSPWSET        No       Password to deactivate RACF still at I
__  10 RVARYSWITCHPWSET        No       Password to switch RACF database still
__   2 TAPEDSN                 No       Tape datasets are unprotected unless T
****************************** BOTTOM OF DATA ********************************
```

Figure 207. SETROPTS settings - audit concerns panel

The display contains the following fields of interest.

Table 166. SETROPTS settings Audit concerns panel - field descriptions

Field	Explanation
Pri	The highest priority for any audit concern for this system.
Complex	The complex name for the security database.
System	The system name.
Count	The number of audit concerns for this system.
Pri	A measure for the severity of the audit concern.
Parameter	The RACF setting that causes the audit concern
Value	The value the parameter is set to.
Audit concern	The audit concern identified for this setting.

Select an audit concern for a detail display.

```
SETROPTS settings - audit concerns                              Line 1 of 12
Command ===>                                                 Scroll===> CSR
                                          30 Aug 2002 10:01
System
Complex name                TODAY
System name                 DINO
SETROPTS setting
Parameter name              OPERAUDIT
Parameter value             No
Audit concern
Relative audit priority     20
Audit concern               OPERATIONS activity undetectable
****************************** BOTTOM OF DATA ********************************
```

RRSFNODE - RACF Remote Sharing Facility settings

The report in Figure 208 on page 271 shows the RACF Remote Sharing Facility nodes properties. The report is generated by a NEWLIST TYPE=RRSFNODE.

The RACF remote sharing facility (RRSF) reports are available on z/OS systems only and require system information. You must supply an input set with a CKFREEZE data source.

```
                RACF remote sharing facility nodes
Command ===> _____________________________________________________ Scroll===> CSR
                                                                    15 Jun 2011 00:07
Complex  System   Local node #Nodes
EEND     EEND     EEND           12
TargNode TargSysn TStat Loc Main Prot LUName   ModeName TPName   Description
__ EEND     EEND     O-A   Yes No   APPC EENDLU01 IRRMODE  IRRRACF  EEND/GANS l
__ DINO              D-L   No  No   APPC DINOLU01 IRRMODE  IRRRACF  RRSF NODE D
__ I522              D-L   No  No   APPC I522LU01 IRRMODE  IRRRACF  RRSF NODE I
__ O110              D-L   No  No   APPC O110LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O130              D-L   No  No   APPC O130LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O240              D-L   No  No   APPC O240LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O250              D-L   No  No   APPC O250LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O260              D-L   No  No   APPC O260LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O270              D-L   No  No   APPC O270LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O280              D-L   No  No   APPC O280LU01 IRRMODE  IRRRACF  RRSF NODE O
__ O290              D-L   No  No   APPC O290LU01 IRRMODE  IRRRACF  RRSF NODE O
__ TREX              D-L   No  No   APPC TREXLU01 IRRMODE  IRRRACF  REMOTE NODE
******************************* Bottom of Data ********************************
```

Figure 208. RRSF node properties

The display includes the following fields.

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Local node	The RRSF local node.
#Node	The number of target nodes.
TargNode	The RRSF node that the local node is connected to.
TargSysn	The MVS (GRS) system name that has the target node as a local node name.
TStat	State of the target RRSF node. For the possible values, see Table 421 on page 1254.
Loc	Flag field (Yes/No) that reflects whether this node is designated as the local node for this system.
Main	Flag field (Yes/No) that reflects whether this node is designated as the main node for this system.
Prot	Protocol for communication. The value can be APPC (Advanced Program-to-Program Communications), or TCPIP (Transmission Control Protocol Internet Protocol).
LUName	Logical unit name for RRSF connection to the target node if using APPC.
ModeName	SNA mode name that designates the network properties to be used when setting the APPC connection to the target node.
TPName	The APPC transaction program profile name (1–64 characters).
Description	Comment describing the target node.
Address	The host name or IP address entered on the TARGET command when defining an RRSF node with TCP protocol.
PortNum	The port number entered on the TARGET command when defining an RRSF node with TCP protocol.

When a node is selected, the detail panel in Figure 209 is displayed. For options not available in your RACF release, no field value is displayed.

```
                RACF remote sharing facility nodes              Line 1 of 25
Command ===> ____________________________________________________ Scroll===> CSR
                                          15 Jun 2011 00:07
Local system
Security complex name         EEND
System name                   EEND
Local node                    EEND

Target node identification            Target node properties
Target node                   EEND    Node is local                 Yes
Target complex                EEND    Node is main                  No
Target system                 EEND    Target state                  O-A
Target sysname                EEND    Protocol                      APPC
Description                   EEND/GANS local (LEN MAX 32)

Workspace data set properties         APPC properties
Workspace SMS Dataclas                APPC LUNAME                   EENDLU01
Workspace SMS Mgmtclas        NONMIG  APPC Mode Name                IRRMODE
Workspace SMS Storclas        STANDARD APPC TP Name                 IRRRACF
Workspace Prefix              EEND
Workspace Qualifier
Workspace Filesize                  500
Workspace Volume

IP properties
Target Node IP Address
Target Node IP Port
****************************** Bottom of Data ********************************
```

Figure 209. RRSF node details display

ROUTER - SAF router table (ICHRFR01)

The information shown in the ROUTER report depends on the level of the operating system that you are reporting about.

On z/OS 1.6 and higher, the report shows the SAF router table (ICHRFR01) as created by the installation. If the installation chose not to create a Router Table for its local resource classes, an empty ROUTER Report can be shown. In that situation, the default action RACF is taken for all RACROUTE requests. This default action is also taken when the installation router table is present, but no matching entry could be located. On z/OS 1.5 and older, this report shows the combination of the IBM router table (ICHRFR0X) and the installation created router table (ICHRFR01).

After selecting or auto-selecting a system on the summary display, the router table for that system is shown. The columns in the report show the priority, class name, requester name, subsystem name, resulting action, and any audit concerns. The action column shows one of the following values:

- *NONE*, if the corresponding RACROUTE requests are not to be passed to RACF.
- *RACF*, if requests are to be passed to RACF.

The audit concern column might show the value `Class not in CDT`. Because the class has not been defined to RACF, ACCESS requests passed to RACF always return the value `not protected`. If the router table indicates that the request should be passed to RACF, the priority is set to 15. If the router table indicates that these requests should not be passed to RACF anyway, the priority is set to 3.

These reports are only available on z/OS systems and require system information. You must supply an input set with one fo the following data sources: `CKFREEZE`

data set, Live system, or active RACF allocation.

```
SAF router table (ICHRFR01)                                    Line 1 of 218
Command ===> ____________________________________________ Scroll===> CSR_
                                                  23 Mar 2005 00:07
   Complex  System   Entries Audit concerns
   DINO     DINO         218             0
Pri Class    Reqstor  Subsys   Act  Audit concern
    ACCTNUM                    RACF
    ACICSPCT                   RACF
    AIMS                       RACF
    ALCSAUTH                   RACF
    APPCLU                     RACF
    APPCPORT                   RACF
    APPCSERV                   RACF
    APPCSERV APPCSDFM APPC/MVS RACF
    APPCSI                     RACF
    APPCSI   APPCSDFM APPC/MVS RACF
    APPCTP                     RACF
    APPCTP   APPCSDFM APPC/MVS RACF
    APPL                       RACF
    BCICSPCT                   RACF
    CACHECLS                   RACF
    CBIND                      RACF
    CCICSCMD                   RACF
    CIMS                       RACF
    CONNECT                    RACF
    CONSOLE                    RACF
    CPSMOBJ                    RACF
    CPSMXMP                    RACF
    CSFKEYS                    RACF
    CSFSERV                    RACF
    DASDVOL                    RACF
    DATASET                    RACF
    DATASET  CLOSE    OCEOV    RACF
    DATASET  TAPEEOV  OCEOV    RACF
    DATASET  TAPEOPEN OCEOV    RACF
    DATASET  TAPERST  RESTART  RACF
```

Figure 210. SAF router display

The table is used for requests passed to SAF (System Authorization Facility) through the RACROUTE macro. If the class is not present, or if ACTION=NONE is contained in the Router Table, the request is not passed to RACF. When a class is not defined in the CDT, RACF flags any references to profiles in such a class as errors, returning a 'class not defined' code.

AUTAB - RACF Authorized Caller Table ICHAUTAB

STATUS AUDIT option AUTAB displays the authorized caller table ICHAUTAB used by RACF. Each line indicates a program name, and flags indicating special authorizations. The authorizations are only granted by RACF if the specified program is loaded from an APF-authorized library (does not need to have AC=1).

These reports are only available on z/OS systems and require system information. You must supply an input set that includes at least one of the following data sources: a CKFREEZE data set, Live system, or active RACF allocation.

Background

The authorized caller table is used to define programs to RACF that are permitted to issue RACLIST (RACROUTE REQUEST=LIST) or RACINIT (RACROUTE REQUEST=VERIFY) calls if only they are loaded from an APF-authorized library. They do not need to be actually APF-authorized (have AC=1).

Auditing the RACF Authorized Caller Table

The authorization to obtain a list of profiles can enable a program to obtain information that it cannot access in any other way.

```
RACF Authorized Caller Table                                    Line 1 of 1
Command ===>                                                   Scroll===> CSR
                                                  29 Jun 1992 06:25
   Complex  System   Entries
   AUTAB    1290           1
Program  RACLIST RACINIT Authorization
AUTH     Yes     No      RACLIST
****************************** BOTTOM OF DATA ********************************
```

Figure 211. Authorized Caller Table display

The display contains the following fields of interest.

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Entries	The number of entries in the table.
Program	The program name.
RACLIST	Program can issue RACLIST, enabling you to obtain access to profiles that would normally be inaccessible.
RACINIT	Program can issue RACINIT without NEWPASS.
Authorization	A text summary of the program's authorizations.

RANGE - RACF Range Table ICHRRNG

The STATUS AUDIT option RANGE leads to a display of the database range table ICHRRNG currently in use by the system. Use the scroll keys to scroll forward and backward through the table.

These reports are only available on z/OS systems and require system information. You must supply an input set that includes data sources: a CKFREEZE data set, Live system, or active RACF allocation.

```
RACF Range Table                                                Line 1 of 7
Command ===>                                                 Scroll===> CSR
                                                 2 Sep 1999 14:49
   Complex  System   Entries
   NDSNOTES ETPS           7
DB# From key (EBCDIC and hexadecimal)
  1
             00000000000000000000000000000000000000000000000000000000000000000000
  2 CR
             C3D90000000000000000000000000000000000000000000000000000000000000000
  1 CS
             C3E20000000000000000000000000000000000000000000000000000000000000000
  3 SYS1
             E2E8E2F10000000000000000000000000000000000000000000000000000000000000
  1 SYS2
             E2E8E2F20000000000000000000000000000000000000000000000000000000000000
  2 USER
             E4E2C5D90000000000000000000000000000000000000000000000000000000000000
  1 VSAMDSET
             E5E2C1D4C4E2C5E30000000000000000000000000000000000000000000000000000
****************************** BOTTOM OF DATA *******************************
```

The range table display shows the RACF data set sequence number and the start key of the range that is directed to this data set. The key is shown both in characters and in hexadecimal representation (though truncated on most terminal types).

RACFDSN - RACF Data Set Name Table ICHRDSNT

The STATUS AUDIT option RACFDSN leads to the data set name table ICHRDSNT display.

These reports are only available on z/OS systems and require system information. You must supply an input set that includes data sources: a CKFREEZE data set, Live system, or active RACF allocation.

Background

The data sets and options used as the RACF database by RACF are initialized from the RACF Data Set Name Table (ICHRDSNT), but can be modified by RVARY commands.

The sequence numbers of the data sets within the database form the basis on which the RACF range table (ICHRRNG) determines which profiles reside in which data set.

Auditing the RACF Data Set Name Table

For each data set sequence number, the primary and duplex data set names are displayed on separate lines:

```
RACF Current database data set names and settings                Line 1 of 6
Command ===>                                                   Scroll===> CSR
                                                    2 Sep 1999 14:49
   Complex  System   Entries
   NDSNOTES ETPS           6
DB# Dataset                                        Volume R/T Buf Attributes
  1 ETP.RACF.PRIMARY.DB1                           ETPSMS  12 255 ShrDASD Act Pri
  1 ETP.RACF.BACKUP.DB1                            ETPSMS  12  51 ShrDASD Act Mst
  2 ETP.RACF.PRIMARY.DB2                           ETPSMS  12 255 ShrDASD Act Pri
  2 ETP.RACF.BACKUP.DB2                            ETPSMS  12  51 ShrDASD Act Dat
  3 ETP.RACF.PRIMARY.DB3                           ETPSMS  12 255 ShrDASD Act Pri
  3 ETP.RACF.BACKUP.DB3                            ETPSMS  12  51 ShrDASD Act Dat
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Table 167. RACF Current database data set names and settings panel - field descriptions

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Entries	The number of entries in the table.
DB#	Database sequence number.
Dataset	Data set name.
Volume	Data set volume serial.
R/T	The number of records per track.
Buf	The number of in-storage buffers (of 1 KB for the non-RDS and 4 KB for the RDS).

Table 167. RACF Current database data set names and settings panel - field descriptions (continued)

Field	Explanation
Attributes	The RACF data set attributes. These are: **DataShare** Data sharing mode active, all other members in IRRXCF00 in data sharing mode or read-only. **DataShareR/O** Read-only mode active, all other members in IRRXCF00 in data sharing mode or read-only. **DataShareTrn** Transition mode. After the connect service completes, the system is in data sharing or read-only mode. **RDS** The data set is in Restructured Data Set format (not shown in RACF releases that only support RDS - 1.9.2 and higher). **ShrDASD** The master data set is on shared DASD. **Act** Data set is active (RACF directs I/O to the data set). **Prim** Data set is primary (RACF directs statistics to the data set). **Mstr** This is the master data set (options & templates in use). **Stat** Statistics should be backed up. **Databuf** The buffer can contain both data and index blocks. **CMS** The data set is in CMS minidisk format

RACFCLAS - Class Descriptor Table report

STATUS AUDIT option CDT displays the class descriptor table ICHERCDE and ICHERCDX as well as the in-storage class activity settings, and profile summaries.

When more than one complex has been setup, the first panel displayed is a summary panel so select the complex:

```
RACF CDT, SETROPTS class info and number of profiles            Line 1 of 2
Command ===>                                                   Scroll===> CSR
                                                  16 Oct 2001 00:07
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
__ C#M4     C#M4         144     44       38     1093             43       23
__ MVS430   B#T          157     79       30      526             43       35
****************************** BOTTOM OF DATA ********************************
```

Figure 212. RACF CDT, SETROPTS class info and number of profiles: Summary screen

Audit concerns are only identified when you have zSecure Audit for ACF2 installed.

After selecting a complex, each class can be selected to display a full overview of the class options currently in effect. The following figure shows the list of classes sorted on audit priority.

```
RACF CDT, SETROPTS class info and number of profiles            Line 1 of 114
Command ===>                                                   Scroll===> CSR
                                                  16 Oct 2001 00:07
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
   C#M4     C#M4         144     44       38     1093              43       23
   Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
__ 22 DEVICES  115                   Inactive                       4      Ye
__  7 DASDVOL   0 GDASDVOL           Inactive                       3  4 OPER Ye
__  5 APPCTP    89                   Inactive                       1  8      Ye
s_  5 APPL       3                   Inactive                       5  4      Ye
__  5 DLFCLASS  92                   Inactive                       2  4      Ye
__  2 DATASET                        Noaudit  Glob                482  4 OPER Ye
__  1 ALCSAUTH 548                   Inactive      Discrete         4 OPER Ye
__  1 APPCSI    88                   Inactive                       4      Ye
__  1 CBIND    545                   Inactive      Discrete         8      Ye
__  1 CPSMOBJ   57 GCPSMOBJ          Inactive                       4      Ye
__  1 CPSMXMP   11                   Inactive                       4      Ye
__  1 DIRECTRY  95                   Inactive      Discrete         8 OPER Ye
__  1 DSNR       7                   Inactive                       4      Ye
__    ACCTNUM  126                                                 2  4      Ye
__    ACICSPCT   5 BCICSPCT                                        4      Ye
__    AIMS       4                   Inactive                       4      Ye
__    APPCLU   118                                                13  4      Ye
__    APPCPORT  87                   Inactive                       4      Ye
__    APPCSERV  84                                                 2  8      Ye
__    BCICSPCT   5          ACICSPCT                               4      Ye
__    CCICSCMD   5 VCICSCMD                                        4      Ye
__    CIMS      93 DIMS               Inactive                     4      Ye
__    CONSOLE  107                                                3  8      Ye
__    CSFKEYS   98 GCSFKEYS          Inactive                       4      Ye
__    CSFSERV   98                   Inactive                       4      Ye
__    DBNFORM   59                   Inactive                       4      Ye
__    DCEUUIDS 544                   Inactive      Discrete         8      Ye
__    DCICSDCT   5 ECICSDCT                                        4      Ye
__    DIMS      93          CIMS     Inactive                     4      Ye
__    DIRACC    71                   Inactive                       8      Ye
__    DIRAUTH  105                   Inactive                       8      Ye
__    DIRSRCH   70                   Inactive                       8      Ye
__    FACILITY   8                                                202  4      Ye
```

Figure 213. RACF CDT, SETROPTS class info sorted by audit priority

The display is designed to show blank columns if the best protection options are used, as much as possible. See the description of CLASS NEWLIST for full documentation on the class options. Table 168 provides a basic description of the columns.

Table 168. RACF CDT, SETROPTS class info and number of profiles report - column descriptions

Pr	Audit priority (filled in only with a zSecure Audit for ACF2 license).
Class	Name of the class in the Class Descriptor Table
Pos	The POSIT number used for determining the options setting for the class. A RACF command which changes class options for any one class also changes these options for all classes with the same POSIT value.
Grouping	This column is filled in for (member) classes that have a related grouping class.
Members	This column is filled in for (grouping) classes that have a related member class.

Table 168. RACF CDT, SETROPTS class info and number of profiles report - column descriptions (continued)

Protect	This column summarizes a number of options. The most 'offensive' option from the security viewpoint is displayed. The priority order for the displayed values is: • Inactive - The class is not active • Noaudit - Profile changes are not audited.

Glbl	This column summarizes the activity of the global access table for the class: ('Global Active') **Glob** Global access checking is active for the class. This does not mean that there are any profiles on the table. **n/a** Global access checking does not apply to this class because the class cannot be combined with SETROPTS RACLIST. This value applies only if you are examining a very old RACF database.

Generic	If generic profiles are not permitted, this column shows the value *Discrete*; Otherwise, this column is blank.
Profiles	Number of profiles in this class.
RC	Default return code. *0* means grant the request as if a profile permittinng access were present. *4* means 'do not know', in which case what happens is application-dependent. *8* means fail the request as if a profile denying access were present.
Oper	This column contains the text `OPER` if the `OPERATIONS` attribute applies to this class. This means that all users with this attribute have access unless specifically denied access.
RFR	Indicates whether the class is present in at least one entry in the SAF router table.
Id	Generic class identifier.
Org	Original sequence number in the Class Descriptor Table.
UACC	Contains the default universal access setting for profiles created in this class. The value can be any of the following: *ALTER*, *CONTROL*, *UPDATE*, *READ*, *NONE*, or *ACEE.* The last value indicates that RACF uses the default `UACC` of the `ACEE` of the user.

Where	Summarizes the options available to regulate profile residency. The following options are available, listed in order of priority: *Nowhere*. The class cannot have any profile which is indicated by `PROFDEF=NO` in the Class Descriptor Table. *RaclReq*. The profiles are resident if the class is active, because RACLIST is required (RACLREQ=YES option in the CDT). *Raclist*. The profiles are resident (by means of the SETROPTS RACLIST option). *Genlist*. The generic profiles are resident (by means of the SETROPTS GENLIST option). *RaclGbo*. The profiles are resident only because they have been RACLISTed by an application via a RACROUTE macro with GLOBAL=YES specified. *NoList*. The profiles cannot be made resident (due to the RACLIST=DISALLOWED and GENLIST=DISALLOWED options in the CDT). This is typically the case for classes meant to be accessed with RACLIST and FRACHECK by applications. *NoRacl*. The profiles are not resident, and only the generic ones can be made resident (by means of SETROPTS GENLIST). Discrete profiles cannot be made resident (due to the RACLIST=DISALLOWED option in the CDT). *NoGenl*. The profiles are not resident, but can be made so (by means of the SETROPTS RACLIST option); however, it is not possible to make only the generic ones resident (due to GENLIST=DISALLOWED in the CDT). (blank) Both generics and discretes or generics only can be made resident by using SETROPTS RACLIST or SETROPTS GENLIST, respectively.

Max	Maximum length of profiles in this class.
MxE	Maximum length for use with the ENTITY keyword of the RACROUTE macro.
Sta	Statistics are collected for this class.
Scl	Security label is required for profiles in this class.
Rvm	Reverse mandatory access checking is required.
EqM	Equal mandatory access checking is required.
Aud	Command auditing is active for this class.
Logopt	Auditing options for this class; can be *Always, Failure, Never, Success*, and *Profile* (determined by the logging options of the profile).
Discrete	Number of discrete profiles in this class.
Generics	Number of generic profiles in this class.
Act	RACF protection is active for this class.
Glb	Global Access Checking is active for this class.
Gen	Generic profile checking for this class is active.
Gcm	Generic commands permitted for this class.
NoP	Profiles cannot be defined in this class.

Gna	This flag field indicates whether SETROPTS GENERIC and SETROPTS GENCMD are permitted for the class.
RlR	A RACLIST is required for this class.
Rcl	The class is RACLISTed (via SETROPTS RACLIST).
Dsp	RACLISTed profiles for this class have been stored in a dataspace.
Gnl	The class is GENLISTed.
GbO	The class is RACLISTed due to RACROUTE GLOBAL=YES only.
RlA	A RACLIST is permitted for this class.
GlA	A GENLIST is permitted for this class.
Sig	An ENF signal must be sent when the class is being RACLISTed, NORACLISTed, or RACLIST refreshed.
Usr	The class is user-installed (as opposed to IBM-defined).
Qu	The number of qualifiers at the start of the profile name that cannot be generic.
Lwr	The profile name can contain lowercase characters.
S1A	The first character of the profile name can be alphabetical.
S1N	The first character of the profile name can be a national character.
S1#	The first character of the profile name can be numerical.
S1S	The first character of the profile name can be a special character.
SRA	The characters after the first character of the profile name can be alphabetical.
SRN	The characters after the first character of the profile name can be national.
SR#	The characters after the first character of the profile name can be numerical.
SRS	The characters after the first character of the profile name can be a special character.
Description	A short explanation of the purpose of the class.
Audit concern	Any audit concerns identified for this class. If you do not have zSecure Audit for ACF2, no attempt is made to identify any.

The following action commands are available.

E - Display event logging

Searches for for SMF events concerning the class it is issued for.

This command starts option **EV.R** General resource events from SMF for the class it is issued for. See “Reporting on general resource events (EV.R)” on page 567.

P - Display profiles

Searches for all defined profiles in the class it is issued for.

It invokes option **RA.R** RESOURCE for the class it is issued for. See “RA.R RESOURCE - General Resource profiles” on page 147.

R - Refresh class

Refreshes the class it is issued for. The generated commands depend on the current settings for the class. See “REFRESH - Automatic refreshes for RACLIST, GENERIC checking, GLOBAL access checking, and WHEN(PROGRAM)” on page 86.

S - Show additional information

Shows additional information about the class it is issued for on the Class Option Display panel. The panel lists all class options set by the CDT and SETROPTS command, the number of profiles in the database of the specified class, and indicates whether the class is present in the SAF router table.

When a class is selected, the class option panel is displayed. Depending on your RACF release, some fields might be blank because the options they represent are not supported by the RACF database.

```
RACF CDT, SETROPTS class info and number of profiles              Line 1 of 35
Command ===> ____________________________________________ Scroll===> CSR_
                                        16 Oct 2001 00:07
  Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
  CRM4     CRM4         144     44       38     1034              0
  Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
     APPL       3                   Inactive                     5  4      Ye


  Description
  Controls access to applications

  Profile syntax rules 1st     rest      Class properties
  Alphabetic allowed   Yes      Yes      Original order (class number)   9
  National allowed     Yes      Yes      Class identifier                8
  Numeric allowed      No       Yes      POSIT (options set id)          3
  Special allowed      No       No       Default UACC                    NONE
  Maximum length                8       Generic scan limit (quals)      0
  Maximum length with ENTITY    8       Installation-defined class      No
  Related grouping class                Profiles names case sensitive No
  Related member class                  Default not-found RC            4

  Class activity options                Profile residency options
  Protection active             No      Profile definition forbidden  No
  GLOBAL (fast path) active     No      Profiles RACLISTed            No
  OPERATIONS honored            No      Profiles in dataspace         No
  Send ENF signal               No      Profiles GENLISTed            No
  Generics checkeded            Yes     RACLIST required              No
  Generics commands allowed     Yes     Profiles may be RACLISTed     Yes
  Generics can be activated     Yes     Profiles may be GENLISTed     Yes
                                        RACLISTed by application only No

  Class audit options                   Mandatory access control properties
  Command auditing active       Yes     SECLABEL required             No
  Statistics collected          No      Reverse MAC checking          No
  Logoptions                    Profile Equal MAC checking            Yes

  RACF database cross-reference         Router table cross-reference
  Number of discretes                5  Class in SAF router table     Yes
  Number of generics
  Number of profiles                 5
******************************* BOTTOM OF DATA ********************************
```

Figure 214. RACF CDT, SETROPTS class info and number of profiles : Class option screen

RACFDCLS - RACF class info from database ICB

STATUS AUDIT option RACFDCLS displays the class info as stored in the RACF database ICB.

```
RACF SETROPTS class info from database ICB                    Line 1 of 128
Command ===> _____________________________________________ Scroll===> CSR
                                          30 Aug 2002 10:19
   Complex  Classes Active Audit concerns Priority
   DINO         128     33              0
   Pr DftClass Pos Protect  Glbl Generic  Sta Logopt   Act Glb Gen Gcm Rcl Gnl

__    ACCTNUM  126                       No  Profile  Yes No  Yes Yes Yes No
__    ALCSAUTH 548 Inactive             No  Profile  No  No  No  No  No  No
__    APPCLU   118                       No  Profile  Yes No  Yes Yes No  No
__    APPCPORT  87                       No  Profile  Yes No  Yes Yes Yes No
__    APPCSERV  84                       No  Profile  Yes No  Yes Yes No  No
__    APPCSI    88 Inactive             No  Profile  No  No  Yes Yes No  No
__    APPCTP    89 Inactive             No  Profile  No  No  Yes Yes No  No
__    APPL       3                      No  Profile  Yes No  Yes Yes No  No
__    CACHECLS 569 Inactive             No  Profile  No  No  No  No  No  No
__    CBIND    545 Inactive             No  Profile  No  No  No  No  No  No
__    CIMS      93 Inactive             No  Profile  No  No  Yes Yes No  No
__    CONSOLE  107                      No  Profile  Yes No  Yes Yes No  No
__    CPSMOBJ   57 Inactive             No  Profile  No  No  Yes Yes No  No
__    CPSMXMP   11 Inactive             No  Profile  No  No  Yes Yes No  No
__    CSFKEYS   99 Inactive             No  Profile  No  No  No  No  No  No
__    DASDVOL    0 Inactive             No  Profile  No  No  Yes Yes No  No
__    DATASET      Noaudit  Glob        No  Profile  Yes Yes Yes Yes No  No
__    DBNFORM   59 Inactive             No  Profile  No  No  Yes Yes No  No
__
```

The columns are designed in such a way that the better the protection options, the less intensified fields are on the display. See the description of the "SETROPTS_CLASS: RACF Class Settings in database" on page 1272 for full documentation of the class options, or call field help by positioning the cursor on the field and pressing PF1.

When a class is selected, the class option panel is displayed. Depending on your RACF release, not all fields can be filled in: options not present in your RACF release are simply left blank.

```
RACF SETROPTS class info from database ICB                      Line 1 of 15
Command ===> _____________________________________________ Scroll===> CSR
                                          30 Aug 2002 10:19
   Complex  Classes Active Audit concerns Priority
   DINO         128     33              0
   Pr DftClass Pos Protect  Glbl Generic  Sta Logopt   Act Glbl Gen Gcm Rcl Gn
      ACCTNUM  126                       No  Profile  Yes      Yes Yes Yes No


  Description
  TSO account numbers

  Class activity options                Class properties
  Protection active             Yes     POSIT (options set id)        126
  GLOBAL (fast path) status     No
  Generics checked              Yes
  Generic commands allowed      Yes

  Profile residency options             Class audit options
  Profiles GENLISTed            No      Statistics collected          No
  Profiles RACLISTed            Yes     Logoptions                    Profile
******************************** BOTTOM OF DATA ********************************
```

GLOBAL - Global Profile overview

STATUS AUDIT option GLOBAL displays the profiles in the GLOBAL class. Each line describes a profile with its owner and universal access level.

```
Global profile overview                                          Line 1 of 3
Command ===> _____________________________________________ Scroll===> CSR
                                              18 Dec 1997 11:39
   Complex  Timestamp        Count
   C#M4     18Dec1997  00:05     3
   Class    Profile  Owner    UACC    ID(*)
__ GLOBAL   DATASET  IBMUSER  NONE
__ GLOBAL   GMBR     C#MBGUS  NONE
__ GLOBAL   INFOMAN  C#MBGUS  NONE
****************************** BOTTOM OF DATA ********************************
```

After selecting one of the profiles, you can see the global access checking entries defined for the class it pertains to, as well as any access list entries for the profile itself.

```
Global profile overview                                          Line 1 of 5
Command ===> _____________________________________________ Scroll===> CSR
                                              18 Dec 1997 11:39
   Complex  Timestamp        Count
   C#M4     18Dec1997  00:05     3
   Class    Profile  Owner    UACC    ID(*)
   GLOBAL   DATASET  IBMUSER  NONE
  Members
  C#MBERT.C#MQA%%%.*/READ
  SYS1.*.ISPCLIB.VB/READ
  SYS1.*.ISP%LIB/READ
  &RACUID.*.**/ALTER
  SYS1.PP.ISP*.**/READ

  User/grp Access
_ CRMXASM  ALTER
****************************** BOTTOM OF DATA ********************************
```

TEMPLATE - Template field properties

The STATUS AUDIT option TEMPLATE lists the field names defined in the RACF database templates together with the default properties assigned by Security zSecure. If an UNLOAD file or a RACF database copy has not been allocated, you must have READ permit access to the RACF data sets to use the TEMPLATE command. You can run the TEMPLATE command from the command line on most Security zSecure panels. Figure 215 on page 285 shows the template display panel.

```
RACF template definitions                                        Line 1 of 317
Command ===>                                                   Scroll===> CSR
                                                    9 Oct 1995 04:14
   Complex  Timestamp          Count
   S0W1      9 Oct 1995  04:14   317
   Entity   Segment  Field     Id Alias-of Group     Bytes Dflt Format   Outlen
__ DATASET  BASE     ENTYPE     2                        1 04   Num           5
__ DATASET  BASE     VERSION    3                        1 01   Hex           2
__ DATASET  BASE     AUTHDATE   4 CREADATE               3 FF   Date         11
__ DATASET  BASE     CREADATE   4                        3 FF   Date         11
__ DATASET  BASE     DEFDATE    4 CREADATE               3 FF   Date         11
__ DATASET  BASE     AUTHOR     5                        8 FF   Char          8
__ DATASET  BASE     OWNER      5 AUTHOR                 8 FF   Char          8
__ DATASET  BASE     LREFDAT    6                        3 FF   Date         11
__ DATASET  BASE     LCHGDAT    7                        3 FF   Date         11
__ DATASET  BASE     ACSALTR    8                        2 FF   Num           5
__ DATASET  BASE     ACSCNTL    9                        2 FF   Num           5
__ DATASET  BASE     ACSUPDT   10                        2 FF   Num           5
__ DATASET  BASE     ACSREAD   11                        2 FF   Num           5
__ DATASET  BASE     UACC      12 UNIVACS                1 00   Access        7
__ DATASET  BASE     UNIVACS   12                        1 00   Access        7
__ DATASET  BASE     FLAG1     13                        1 00   Flag          3
__ DATASET  BASE     AUDIT     14                        1 00   Audit         7
__ DATASET  BASE     GROUPNM   15                        8 FF   Char          8
__ DATASET  BASE     DSTYPE    16                        1 00   DsType        5
__ DATASET  BASE     LEVEL     17                        1 FF   Num           5
__ DATASET  BASE     DEVTYP    18                        4 FF   Hex           8
__ DATASET  BASE     DEVTYPX   19                        8 FF   Char          8
__ DATASET  BASE     GAUDIT    20                        1 00   Audit         7
__ DATASET  BASE     INSTDATA  21                   Varies 00   Char         44
__ DATASET  BASE     AUDITQS   22                        1 FF   AudLvl        7
__ DATASET  BASE     AUDITQF   23                        1 FF   AudLvl        7
__ DATASET  BASE     GAUDITQS  24                        1 FF   AudLvl        7
__ DATASET  BASE     GAUDITQF  25                        1 FF   AudLvl        7
__ DATASET  BASE     WARNING   26                        1 00   Flag          3
__ DATASET  BASE     SECLEVEL  27                        1 FF   Seclevel      8
__ DATASET  BASE     NUMCTGY   28                        4 00   Num           5
__ DATASET  BASE     CATEGORY  29          NUMCTGY       2 00   Category      8
__ DATASET  BASE     NOTIFY    30                   Varies 00   Char          8
__ DATASET  BASE     RETPD     31                   Varies 00   $retpd        5
```

Figure 215. RACF template definitions display panel

The Template Display shows one line per template or custom field. The first three columns, Entity, Segment, and Field, uniquely identify a field. Entity and Id also uniquely identify a field. The display shows columns that directly reflect fields in the template in the master database, as well as columns with a Security zSecure interpretation. You can scroll left/right and up/down to see all fields and columns. To view a detail display of any field, use the **S** line command to select it.

Table 169 describes the fields included in the Template display.

Table 169. RACF template definitions display panel - field descriptions

Entity	Name of the entity type . This can be GROUP (1), USER (2), CONNECT (3 - non-RDS only), DATASET (4), or GENERAL (5). Classes for entity type GENERAL are further defined in the Class Descriptor Table. The other entity types are reserved.
Segment	Name of the segment containing the field. The base segment can be displayed as `BASE` as well as `Base`. The latter syntax indicates that the field lies in a different segment as far as the templates are concerned for a non-RDS (see APAR OY41581, for example).
Field	The name of the field. You can use this name as a parameter on the SELECT, EXCLUDE, LIST, SORTLIST, DISPLAY, and (D)SUMMARY commands.

Table 169. RACF template definitions display panel - field descriptions (continued)

Id	Number indicating the field id from an RDS-template. The **Id** field is the key field used in the internal representation of the profile to locate a field in a profile. For non-RDS, this value is generated by Security zSecure.
Alias-of	Identifies the field as an alias name for another field. You can use alias field names anywhere in Security zSecure. (The template also has combination fields that identify a combination of fields, but these are not displayed because they are not used by Security zSecure.) The internal template information columns are not filled in for aliases since the template does not contain them.
Group	Name of the count field of the repeat group that contains the field. This name is used by Security zSecure to identify a repeat group.
Bytes	This column gives the field length as it is contained in the template. For fields of varying length, this column displays the value `Varies`.
Dflt	The default value from the template (RDS-only). It shows the value returned by RACF for a field if it is not physically present in the profile.
Format	The default output format used by Security zSecure to display or print the field. If it is blank, the field is displayed *as is*.
Outlen	Default length of the field on output produced by Security zSecure. If this field contains `the value Varies`, there is no default length and list/display produces a ragged column layout unless you provide an overriding length.
Mask	This column shows whether the field is masked or encrypted by default by RACF.
Stat	This column shows whether the field is a statistic.
Sort	This column shows whether the field is stored in sorted order in the template (RDS only).
Pad	Field should be padded with binary zeros on the left side.
VLF	Field is eligible for caching in VLF.
AIM	This column shows whether the field is an Application Identity Mapping alias name
EBC	This column shows for an AIM alias name field whether it contains EBCDIC values
Cnf	This column shows whether the field is confidential (not unloaded)
Dt3	This column shows whether the field contains a 3-byte date
Tmp	The field name is represented in the templates.
DPI	The field name is present as a keyword name in the RACF Dynamic Parse Table.
Sy1	The character set for the first character of a field value.
Sy0	The character set for characters beyond the first.
Mix	The maximum length that can be input for the field.
Maxlen	The maximum length that can be input for the field.
Minval	The minimum value for a numeric field.
Maxval	The maximum value for a numeric field.
Header default	Default column header for LIST family of commands.
Command parm	The parameter used to set or change the value of the field with RACF commands.

Table 169. RACF template definitions display panel - field descriptions (continued)

Command parm fmt	The format to be used for the value of the field when generating RACF commands.
Description	Default prefix header for LIST family of commands.

This panel supports the same commands as in any display panel, SORT, FIND for example.

When you select any row with an **S**, all available information about the field is displayed in a Template Detail panel.

```
RACF template definitions                                      Line 1 of 27
Command ===>                                                 Scroll===> CSR
                                              9 Oct 1995 04:14

 Field identification
 Field name                    CGFLAG1
 Type of profile               USER
 Segment containing field      BASE
 Sequence number               58
 Security complex name         S0W1
 Database time stamp            9 Oct 1995 04:14

 Template definitions
 Field defined in template     Yes
 Field name referred to
 Size in bytes                 1
 Default value (hex)           00
 Masked-field flag             No
 Statistic-field flag          No
 Sorted-field flag             No
 Pad-field flag                No
 VLF flag                      Yes
 Field is indexed alias name   No
 Alias name is in EBCDIC
 Forbid unload (confidential)  No
 Contains a 3-byte date        No

Dynamic parse information
Field has dynamic parse info  No
RACF help text
Syntax of first character
Syntax of other characters
Minimum field value
Maximum field value

 Template interpretation
 Group-count field             CGGRPCT
 Default output format         Flag
 Default output length         3
 Maximum input length
 Preserve mixed case           No
 Default output header         gAP
 Command operand
 Command operand format
 Main use for this field       Group ADSP attribute
```

You can obtain a full listing of the RACF database templates for a z/OS system using the primary command **TEMPLATE** or the TEMPLATE option available by selecting the RACF Control option on the Audit Status panel (**AU.S**). See "TEMPLATE - Template field properties" on page 284.

STCTABLE - Started Procedure Table and Started Class

STATUS AUDIT option STCTABLE provides details about the identity and level of trust with which the started tasks in the system run. Two displays are provided: One showing the profiles in the started class (STARTED) and one showing the started procedure table ICHRIN03 currently in use (STCTABLE).

These reports are only available on z/OS systems. Because the reports need system information, you need to select an input an input set with a CKFREEZE data set, live system, or active RACF allocation.

Background

When a START command is issued at the console or through the MGCR SVC (SVC 34), RACF 2.1 and up first look for an applicable profile in the STARTED class. With an earlier RACF release, or when no matching profile is found, the started procedure table is checked.

If a match is found, RACF tries to RACINIT with the specified USER and GROUP (if specified). If the user/group combination is invalid, then the started task runs under the default user and group (user * and group * in the ACEE and ++++++++ [2] in the user token. Note that RACF does not look for another match.

The Started Procedure Table simply contains a list of procedure names. The Started Class provides additional granularity by using profiles with two qualifiers (`procedure.jobname`). Each of these qualifiers can be generic. The Started Procedure Table contains discretes, but can contain the entry *.

To match RACF definitions and tables against the actual procedure libraries, see the RACF RESOURCE category report discussed in “STCPROT - Started Task protection report” on page 344 and “Finding inconsistencies in started task definitions” on page 367.

For more information on started task processing, including the STARTED class, see the REPORT STC command (which reports on started task processing) and the VERIFY STC command (which indicates errors in started task definitions). They are described in “REPORT” on page 875 and “VERIFY” on page 942.

STARTED - Auditing the Started Class

The Started Class profiles are a means to provide a RACF identity (user and group) to a started task, and additionally specify whether the task should run privileged or trusted.

Clearly, each task in the system should have a matching entry, and special care should be taken with respect to generic catchalls. A catchall is wanted to avoid a fallback to the Started Procedure Table.

A *.* entry in the Started Class should preferably have a specification =MEMBER for either user or group (but not both). Such an entry ensures that the SPT is not used unless the Started Class is inactive. For such an eventuality it can be wise to have a few SPT entries to ensure the system can at least IPL reasonably.

---

2. The value '++++++++' is the default for the JES undefined user; the actual value is reported in the SETROPTS report in “SETROPTS - RACF settings report” on page 266 under the heading "Job Entry Subsystem options" as "Default uid local UNDEFINEDU", and is generally available in the UNDEFINEDUSER field of the SYSTEM NEWLIST

The STARTED display shows the profiles in the started class. Each line indicates a profile (consisting of two qualifiers, the first indicating the started task name), and the user and group names that are assigned by RACF.

```
RACF Profiles in Started Class - sorted by procedure            Line 1 of 60
Command ===>                                                  Scroll===> CSR
                                              18 Dec 1997 11:54

   Complex  Timestamp        Count
   C#M4     18Dec1997  00:05    60
   Profile key       Userid   Group    Pri Tru Tra
__ ANTMAIN.*         STRTASK  SYS1
__ APPC.*            STRTASK  SYS1         YES
__ ASCH.*            STRTASK  SYS1         YES
__ ASCHINT.*         STRTASK  SYS1         YES
__ BLSJPRMI.*        STRTASK  SYS1         YES
__ CATALOG.*         STRTASK  SYS1         YES
__ CIC410A.*         CIC410A  STCUSER
__ CIC410B.*         CIC410B  STCUSER
__ CNF#SMS.*         STRTASK  SYSAPPL
__ CNRUNL.*          STRTASK  SYSAPPL
```

Figure 216. STARTED class by procedure

The following fields of interest are shown.

Field	Description
Profile key	The profile name (two qualifiers, each of which can be *).
Userid	The user a matching task should run under.
Group	The group a matching task should run under.
Pri Tru Tra	Should the task run privileged, run trusted, be traced (see below).

The last three columns display flags. These are important since they alter the way RACF processes requests for these started tasks.

Pri	Privileged, for example, all authorization requests are honored without Audit trail.
Tru	Trusted, for example, all authorization requests are honored but with Audit trail.
Tra	Traced, for example, RACF issues message IRR812I when the profile and started procedure are used.

On the detail display, the following extra information about the user profile is shown.

Field	Description
Name	The name field of the user profile.
InstData	The installation data field of the user profile.

STCTABLE - Auditing the Started Procedure Table

Use the Started Procedure Table to provide a RACF identity (user and group) for a started task and also specify whether to run the task using a privileged or trusted access level. You can also perform these functions using the Started Class.

If you use the Started Procedure Table, each task in the system requires a matching entry. You can use an SPT entry with the contents * = STCGRP. The group name (STCGROUP) is a group reserved for holding started task user IDs for an environment that has *list-of-groups checking* configured. For more information, see the *Security Server RACF System Programmer's Guide*.

To safeguard against the eventuality that the Started Class is inactive, create several SPT entries so that the system can restart with one of the other entries.

The STCTABLE display shows the started procedure table ICHRIN03 currently in use. Each line indicates a procedure name, and the user and group names that are assigned by RACF.

```
RACF Started Procedure Table - sorted by procedure      Line 1 of 34
Command ===> _____________________________________________ Scroll===> CSR
                                              30 Apr 1994 05:30
   Complex  System   Count
   RC94     T#D1        34
   Procname Userid   Group    Attr
__ *        =
__ CNMAPRC  SYSCNM   SYSSTC
__ CNMASSI  SYSCNM   SYSSTC
__ CNMPROC  SYSCNM   SYSSTC
__ CNMPSSI  SYSCNM   SYSSTC
__ CNMTPRC  SYSCNM   SYSSTC
__ CNMTSSI  SYSCNM   SYSSTC
__ DFHSM    SYSHSM   SYSSTOR
__ DFHSMABR SYSHSM   SYSSTOR
__ DUMP     RCBBDMP  SYSOPR
__ EREP     SYSEREP  SYSOPR
s_ IDMSAPPL RCAO000  RCAO
__ JESA     SYSJES2  SYSSTC   Privileged
__ JESB     SYSJES2  SYSSTC   Privileged
__ JESC     SYSJES2  SYSSTC   Privileged
__ LEEGDUMP RCBBMAN  SYSOPR
__ NETCNTL  RCAO000  RCAO
__ PRODCNTL RCAO000  RCAO
__ PSF      SYSJES2  SYSSTC
__ RACF     IBMUSER  SYS1
__ RACFIN1  IBMUSER  SYS1
__ RACFIN2  IBMUSER  SYS1
__ RCBBMAN  RCBBMAN  SYSOPR
__ RCCSRMF  RCCSRMF  SYSOPR
__ REST     RCBBRST  SYSOPR
__ RMF      RCCSRMF  SYSOPR
__ RMFGAT   RCCSRMF  SYSOPR
__ SYSPSF1  SYSJES2  SYSSTC   Privileged
__ TCAS     SYSTCAS  SYSSTC   Privileged
__ VTAMAPPL RCAO000  RCAO
__ VTAMINIT RCAO000  RCAO
__ VTAMTUDT SYSVTAM  SYSSTC   Privileged
__ VTAMTUD1 SYSVTAM  SYSSTC   Privileged
__ VTAMUITW SYSVTAM  SYSSTC   Privileged
****************************** BOTTOM OF DATA ******************************
```

Figure 217. SPT overview display

The entries are initially shown in alphabetical order. If a generic entry is defined, this is displayed as the line with * as procedure name.

The following fields of interest are shown.

Field	Description
Procname	The procedure name (or the generic entry *). The report has been sorted on this column, so the generic entry is up front.
Userid	The user a matching procedure should run under.
Group	The group a matching procedure should run under.
Attr	Whether the procedure should run privileged or trusted.

The last column displays flags. These are important, since they alter the way RACF processes requests for these started tasks.

Privileged	All authorization requests are honored without Audit trail.
Trusted	All authorization requests are honored but with Audit trail.

Any of the entries can be selected to view detail information of the started task `userid`.

```
RACF Started Procedure Table - sorted by procedure              Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR
                                          30 Apr 1994 05:30
   Complex  System   Count
   RC94     T#D1        34
   Procname Userid   Group    Attr
   IDMSAPPL RCAO0000  RCAO
  Userid   Name                 InstData
_ RCAO0000  NETVIEW AUTOTASK
****************************** BOTTOM OF DATA ********************************
```

Figure 218. SPT detail display

In addition, the detail display provides the following information about the user profile.

Name	The name field of the user profile
InstData	The installation data field of the user profile.

STATUS AUDIT - RACF user

This section describes RACF reports on RACF users, detailing special authorizations, password settings and usage, and logons. They generally generate a lot of output, and the TRUSTUSR report requires a full CKFREEZE read. The TRUSTUSR report shows which users could compromise the system because they have sensitive access to the Trusted Computing Base.

More RACF reports are available in the CARLa library or from the main menu options **RA** and **AU.V**. You are advised to run the collection batch report `CKRL$ALL`, which includes other reports, at least once.

The following RACF reports are described in this section:

- TRUSTUSR - Trusted users report
- AUTHSYS - System Authorization reports
- AUTHGRP - Group Authorization report
- SHRDUIDS - Shared UNIX uids and gids reports

- PWINLONG - Exceptional Password Interval reports
- PWEXPIRE - Expired Password report
- PWNOCHG - Initial Password report
- PWAGE - Password and Password Phrase Age reports
- PWTRIES - Failed Logon Attempts report
- LGNEVER - Never Used Userids reports
- LGREVOKE - Inactive Userids report
- LGAGE - Last Logon Date reports

TRUSTUSR - Trusted users report

This report shows the access of users to sensitive resources, grouped by user. A similar report grouped by sensitive resource is “SENSTRUS - Sensitive Data Trustees report” on page 317.

Background

A common audit function is to review who can compromise sensitive resources. For some data sets, updates must be tightly controlled (like , APF data sets, and page/swap data sets). For other data sets read access to the information must be tightly controlled (like the RACF database and page/swap data sets). In Security zSecure, resources are called 'sensitive' if access to them can be used directly or indirectly to bypass normal system security. Users that have such access are called 'trusted'. If a hacker wants to bypass the normal security controls, it is sufficient for him to guess, sniff, or steal the password of any of the trusted `userids`.

Auditing trusted users

The trusted users report can be customized to consider JES2 proclibs used for batch jobs sensitive by checking the 'JES2 JOB proclibs considered sensitive' option on the customization panel of the STATUS AUDIT menu. In a batch job you can achieve the same effect by including the CARLa command SIMULATE SENSITIVE PROCLIB.

A sample display is shown in the following figure.

```
Trusted userids (may bypass security)                          Line 1 of 119
Command ===> _____________________________________________ Scroll===> CSR_
                                              8 Sep 2000 00:07
   Pri Complex  Trusted userids
    10 TODAY               119
   Pri Reasons Userid   Name                 RIP DfltGrp  InstData
__  10     253 C##BERT  ERIC TWAIN              SYSPROG
__  10     250 C##BMR1  MARK ROSE               SYSPROG  INSTDATA
__  10     239 C##BPK2  PAUL KING               SYSPROG
__  10     199 R##SLIN  LINDA NEWMAN SPEC.      SYSPROG
__  10     190 C##BPK1  PAUL KING SPEC.         SYSPROG
__  10     184 SYSPSTC  STC USER SYSPROG        SYSPROG
s_  10      96 STRTASK  DIV STARTED TASK USR    SYS1
__  10      42 C##BER2  ERIC TWAIN              C##B
__  10      42 C##BMR2  MARK ROSE B             C##B     TEST INSTA
__  10      42 C##QARUN USER RUNT TESTS         C##QA    ONDER DEZE USER LOPEN
__  10      37 C##BER4  ERIC TWAIN ¬OMVS        C##B
__  10      10 WEBSRV                           IMWEB    ADDED BY INSTALL OS39
__  10       8 BPXOINIT 01234567890123456890  I SYSAPPL
__  10       8 OMVS                            SYSAPPL
__  10       7 DSNASTC  DB2 STC USERID       RI OMVSGRP
__  10       7 OMVSKERN                        OMVSGRP
__  10       4 C##QAN24 REVOKED FOR QR71113  RI C##QA    REVOKED USER FOR QR71
__  10       4 C##QA1S  QA SUBJECT + SPECIAL    C##QA
__  10       3 C##BQAC4                        C##BQA   SURROGAT USER TO SUBM
__  10       3 C##QAP   PROTERM QA TEST USER    C##QA
__  10       3 C##QA001 QA SUBJECT 001          C##QA
__  10       3 C##QA1G  QA SUBJECT + GRPSPEC    C##QA
__  10       2 C@@QA000 CVO TEST SPECIAL        C@@QA    ONDER DEZE USER CVO S
__  10       1 C##QA014 QA SUBJECT 014       R  C##QA
__  10       1 C@@QA001 CVO TEST GROUP SPECI    C@@QA    ONDER DEZE USER CVO G
__  10       1 C@@QA010 TST                  R P C@@QA    TEST FOR CVO
__  10       1 C@@QA011 CVO TEST SUBJECT     R  C@@QA    CVO TEST SUBJECT
__  10       1 C@@QA012 CVO TEST SUBJECT     R  C@@QA    CVO TEST SUBJECT
__  10       1 C@@QRUN  CVO TEST RUNNER         C@@QA    SUBMITS CVO TESTS
__   9      61 C##AINT  Zsecur GROUP ADMIN      C##BEPRD
```

The display contains the following fields of interest.

Field	Description
Pri	The highest audit priority found for the complex
Complex	The complex name for the security database.
Trusted userids	The number of trusted users
Pri	The highest audit priority for this sensitivity type
Reasons	The number of reasons that make the user trusted
Userid	The trusted `userid`
Name	The name of the user
RIP	The flags Revoked, Inactive, and Protected
Dfltgrp	The user's default group
InstData	The user's installation data

Select any `userid` for a list of audit concerns.

```
Trusted userids (may bypass security)                          Line 1 of 33
Command ===> ____________________________________________ Scroll===> CSR_
                                          8 Sep 2000 00:07
   Pri Complex  Trusted userids
    10 TODAY               119
   Pri Reasons Userid   Name                RIP DfltGrp  InstData
    10      96 STRTASK  DIV STARTED TASK USR     SYS1
   Pri Cnt Audit concern
__  10   1 Can use Trojan attacks via the homedirectory of trusted user C##BMR1
__  10   1 Can use Trojan attacks via the homedirectory of trusted user OMVS
__   9   1 JCL that runs with high authority may be changed
__   9   1 May change APF program that can bypass security
__   9   1 Security-relevant parameters may be changed
__   8   1 Can alter the RMM control data set, thus gaining access to any tape.
__   8   1 Can use Trojan attacks via the homedirectory of trusted user BPXOINI
__   8   1 UID(0) user can write any file
__   7   2 May mark jobs as propagated from any user
__   6   1 Can grant HSM USER authority to any user
__   6   2 Can dump all data sets, gaining access
__   6   2 Can dump and delete all data sets, gaining access
__   6   2 Can print all data sets, gaining access
__   6   2 Can rename all data sets, gaining access
__   6   2 Can restore and rename all data sets, gaining access
__   5   1 Can restore and then read any data set without security check
s_   4   2 Dictionary or brute force password attack possible against all users
__   4   2 May contain readable passwords
__   4   3 May contain readable passwords and other confidential data
__   4   3 SMF often contains passwords typed instead of userids
__   4  22 Can change RACF commands in transit via RRSF
__   3   1 Can use Trojan attacks by changing trusted user BPXOINIT's command h
__   3   1 Can use Trojan attacks by changing trusted user C##BMR1's command hi
__   3   1 Can use Trojan attacks by changing trusted user OMVS's command histo
__   3   2 Can copy all data sets. Possibly to readable volume
__   3   2 Can move all data sets. Possibly to an accessible location
__   3   2 Can restore all data sets, possibly to an accessible location
__   3   3 Can restore confidential data by changing DASD management administra
__   2   1 Can update a job to use the current (possibly changed) linklist
__   2   3 Audit trail in SMF may be falsified
__   2   3 Can compromise system by changing SMS settings
__   2  22 Dictionary or brute force password attack possible against users of RRSF
__   1   1 Dictionary or brute force password attack possible against all users
****************************** BOTTOM OF DATA *******************************
```

The display contains the following fields of interest

Field	Description
Pri	The highest audit priority for this user/resource pair.
Cnt	The number of resources to which this concern applies.
Audit concern	An explanation of the risk.

Select any audit concern to view the resources at risk.

```
Trusted userids (may bypass security)                          Line 1 of 2
Command ===> ____________________________________________ Scroll===> CSR_
                                          8 Sep 2000 00:07
   Pri Complex  Trusted userids
    10 TODAY               119
   Pri Reasons Userid   Name                RIP DfltGrp  InstData
    10      96 STRTASK  DIV STARTED TASK USR     SYS1
   Pri Cnt Audit concern
     4   2 Dictionary or brute force password attack possible against all users
   Pri Complex  Sensitivity Resource                                  Risk
__   4 TODAY    RACF back   SYSS.RACF.BACKUP                          READ
s_   4 TODAY    RACF prim   SYSS.RACF.PRIMARY                         READ
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Field	Description
Pri	The audit priority for this user/resource/profile triple.
Complex	The complex for the system that can be attacked.
Sensitivity	The type of sensitivity of the resource on the system at risk
Resource	The name of the resource
Risk	The access level that makes one trusted.
Profile	The profile key in the user's complex covering the resource.
Access	The access level granted to the user on the user's complex.
Via	The group id that grants the user access (when access is given via a group.)

Select any resource for a detail display.

```
Trusted userids (may bypass security)                          Line 1 of 26
Command ===> _____________________________________________ Scroll===> CSR_
                                          5 Feb 2004 17:10


  Trusted subject
  Complex used for the attack   TODAY
_ Trusted userid                STRTASK  DIV STARTED TASK USR
  Revoked (may be by date)
  Inactive, revoked or pending
  Password disabled   PROTECTED

  Subject capability
  Privilege on user's complex   PermitGrp
_ Id associated with privilege  SYSPROG
  Access level granted to user  READ
  RACF profile class            DATASET
  RACF profile                  SYSS.RACF.**
  Relative audit priority       4
  Audit concern                 Dictionary or brute force password attack
  Audit concern                 possible against all users

  Sensitive object user may compromise
  Access level that is exposure READ
  Type of sensitive resource    RACF prim
_ Resource class                DATASET
  Resource name                 SYSS.RACF.PRIMARY
  Volume serial for resource    SHR000
_ System that may be attacked   DINO
  Complex that may be attacked  TODAY
****************************** BOTTOM OF DATA *******************************
```

The display contains the following fields of interest.

Field	Description
Complex used for the attack	The complex where the trusted userid is defined.
Trusted userid	The trusted `userid` followed by the user name and instdata for that ID.
Revoked (may be by date)	Whether the `userid` is revoked. This is determined by the evaluating the revoke flag and the revoke and resume dates.
Inactive, revoked or pending	Whether the `userid` can be revoked due to the `SETROPTS INACTIVE()` setting if the user logged on now.
Password disabled PROTECTED	Indicates whether the `userid` is protected so that it cannot be used for logging on to the system.
Privilege on user's complex	The privilege, security attribute, or operating system function granting the user access.
Id associated with privilege	The group id that grants the user access (when access is given via a group.)
Access level granted to user	The access granted if applicable to the privilege.
RACF profile class	The class of the profile which grants access, or an identifier which describes the domain of the privilege.
RACF profile	The RACF profile covering the resource.
Relative audit priority	A measure for the risk the privilege poses
Audit concern	Explanation how the privilege can be used to obtain the highest system authorization. It can be further annotated for higher priorities.

Field	Description
Access level that is exposure	The minimum access level making a `userid` trusted.
Type of sensitive resource	The type of sensitivity the resource has.
Resource class	The resource class (if applicable).
Resource name	The resource name (if applicable).
Volume serial for resource	Volume serial if relevant for object identification
System that can be attacked	The target system where the resource resides
Complex that may be attacked	The target complex. This value can differ from the complex with the subject and permissive security rule.

In this particular example, user `STRTASK` has `READ` access because of a `PERMIT` (access list entry) for a group to a `DATASET` profile that protects the (primary) RACF database, which contains encrypted passwords. Therefore, this user could try to break a password by encrypting candidate passwords and comparing the results to the value stored in the database.

AUTHSYS - System Authorization reports

These reports show the users that have system-wide special, operations, auditor, or class authorization, or have uid 0 (UNIX superuser authority).

The AUTHSYS report shows the users with system-wide special, operations, auditor, or class authorization. The AUTHUID0 report shows the users with uid 0 in z/OS UNIX.

A sample display for the AUTHSYS report is shown in the following figure.

```
Users with system-wide special, operations, auditor,              Line 1 of 27
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp        System authorized Special Operations Auditor ClAut
   DINO     7May2001  00:07               27       7          4      12    12
   Userid   Name                 Owner    RIRP SOA ClassAut LastUseDa LastPwdCh
s_ AUTMULTI TWO CLASS ADMIN      AUTH             <more>   28Apr2001 20Apr2001
__ AUTPROG  PROGRAM CLASS ADMIN  AUTH             PROGRAM  09Mar2001 09Mar2001
__ AUTSPEC  SYSTEM SPECIAL       AUTH          Y           23Feb2001 23Feb2001
__ AUTSPEC2 ANOTHER SPECIAL      AUTH          Y           09Mar2001 02Sep1997
__ AUTXTA   SPECIAL OPERATIONS   AUTH     Y    YY          10Nov1998 02Jan1998
```

The display contains the following fields of interest.

Field	Description
Complex	The complex name for the security database.
Timestamp	The date and time to which the information pertains.
System authorized	The number of users that have system-wide authorization.
Special	The number of users that are (system-wide) special.
Operations	The number of users that are (system-wide) operations.
Auditor	The number of users that are (system-wide) auditor.

Field	Description
ClAut	The number of users that have class authorization.
Userid	The ID for the user.
Name	The user name.
Owner	The owner of the `userid`.
RIRP	The flags Revoked, Inactive, Restricted (user has no access via GAC, UACC, and ID(*)), and Protected (user cannot logon).
SOA	The flags Special, Operations, Auditor (user has system authority).
ClassAut	The class the user is authorized for. In case of <more> than one such class, view the detail display for the list.
LastUseDa	The date of the user's last logon.
LastPwdCh	The date of the user's last password change.
LastPhrCh	The user's last password phrase change date.
InstData	Installation data field of the user profile.

The detail display lists all classes the user has class authorization for.

```
Users with system-wide special, operations, auditor,              Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp        System authorized Special Operations Auditor ClAut
   DINO     7May2001  00:07                 27       7          4      12    12
   Userid   Name                 Owner    RIRP SOA ClassAut LastUseDa LastPwdCh
   AUTMULTI TWO CLASS ADMIN      AUTH             <more>   28Apr2001 20Apr2001
  ClassAut
  USER
  FACILITY
****************************** BOTTOM OF DATA ********************************
```

A sample display for the AUTHUID0 report is shown in the following figure.

```
Users with uid 0                                                  Line 1 of 7
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp        Users with uid 0
   DINO     7May2001  00:07                 8
   Userid   OMVS uid   Name                 Owner    RIRP SOA LastConDa LastPwd
__ BPXOINIT          0 01234567890123456890 SYSAPPL   Y
__ C##BMR1           0 MARK ROSE            C##B          YYY 04May2001 25Apr20
__ DSNASTC           0 DB2 STC USERID       STCUSER  YY       31Aug1999 29Mar19
__ OMVS              0                      SYSAPPL          06May2001
__ OMVSKERN          0                      OMVSGRP  Y       09May2000
__ STRTASK           0 DIV STARTED TASK USR SYS1             07May2001
__ WEBSRV            0                      R##SLIN  Y       10May2000
****************************** BOTTOM OF DATA ********************************
```

The display contains the following field of interest.

Field	Description
Complex	The complex name.
Timestamp	The date and time to which the information pertains.
User with uid 0	The number of users with `UID= 0` in z/OS UNIX.

Field	Description
Userid	The RACF user ID.
OMVS uid	The UNIX UID (0). Shown to permit overtype in zSecure Admin.
Name	The user name
Owner	The owner of the userid
RIRP	Flag fields indicating the current setting for the following status values: • Inactive • Revoked • Restricted–user has no access through the GAC, UACC, and ID(*)). • Protected–user cannot logon).
SOA	The flags Special, Operations, Auditor (system authorities).
LastConDa	The date of the user's last logon current connect groups.
LastPwdCh	The date of the user's last password change.
LastPhrCh	The user's last password phrase change date.
InstData	Installation data field of the user profile

On the detail display, the **InstData** field is shown wrapped to the screen width.

AUTHGRP - Group Authorization report

This report shows user with group-special, group-operations, or group-auditor authorization. A sample display is shown in the following figure.

```
Users with group level special, operations, auditor              Line 1 of 30
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp        Group authorized Grpspecial Grpoper Grpauditor
   DINO     7May2001  00:07               30         23       6          9
   Userid   Name                 Owner    RIRP soa LastUse LastPwd LastPhr Inst
s_ C#MCXGS  GRPSPEC TEST USER    C#MCXGRP  Y   Y   28Apr01 20Apr01
__ C#MCX01  TEST USER, NO TSO    C#MC      Y     Y 27Apr01 09Apr01
__ C#MQARUN USER RUNS TESTS      C#MQA         Y   06May01 25Feb01
__ C#MQA002 QA SUBJECT DUAL AUTH C#MQA         YYY 02Apr01 08Mar01
```

The display contains the following fields of interest.

Field	Description
Complex	The complex name for the security database.
Timestamp	The date and time to which the information pertains.
Group authorized	The number of users that have group-level authorization.
Grpspecial	The number of users that are group-special.
Grpoper	The number of users that are group-operations.
Grpauditor	The number of users that are group-auditor.
Userid	The userid.
Name	The user name.
Owner	The owner of the userid.

Field	Description
RIRP	The flags Revoked, Inactive, Restricted (user has no access via GAC, UACC, and ID(*)), and Protected (user cannot logon)
soa	The flags group-special, group-operations, and group-auditor.
LastUse	The date of the user's last logon.
LastPwd	The date of the user's last password change.
LastPhr	The user's last password phrase change date.
InstData	Installation data field of the user profile.

Note that this is the only display to list "soa" (group-level) instead of "SOA" (system-wide) on the record level.

The detail display lists the user's authorized connections.

```
Users with group level special, operations, auditor               Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp        Group authorized Grpspecial Grpoper Grpauditor
   DINO     7May2001  00:07              30         23       6          9
   Userid   Name                 Owner    RIRP soa LastUse LastPwd LastPhr Inst
   C#MCXGS  GRPSPEC TEST USER    C#MCXGRP  Y   Y   28Apr01 20Apr01
  User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt
  C#MCXGRP USE       S      NONE
****************************** BOTTOM OF DATA ********************************
```

The detail display lists for each of the user's authorized connections:

Field	Description
User/grp	The group the user is connected to.
Auth	The authority of the connection.
R	Whether the connection is Revoked.
SOA	The group-special, group-operations, and group-auditor flags
AG	The ADSP and Group access flags.
Uacc	The universal access level.
Revokedt	Revoke date for the connection
Resumedt	Resume date for the connection

SHRDUIDS - Shared UNIX uids and gids reports

These reports show what uids and gids (which should preferably be unique, since they are the level at which UNIX security is regulated) are shared by several users or groups.

The SHRDUIDS reports show the uids shared by multiple users. The OMVSNUID report shows the users that have an OMVS segment but do not have a uid assigned. The SHRDGIDS report shows the gids shared by multiple groups. The OMVSNGID report shows the groups that have an OMVS segment but do not have a gid assigned.

A sample display for the SHRDUIDS report is shown in the following figure.

```
OMVS UIDs shared between RACF users                              Line 1 of 14
Command ===> _____________________________________________ Scroll===> CSR_
                                                  12 Sep 2000 00:07
   Complex  Timestamp  Shared uids
   TODAY    12Sep2000           14
            OMVS uid   Occurrences
__                  0           7
__                  2           3
__                110           2
__               4321           2
s_               5999           2
__               7003           2
__               7005           2
__               7012           2
__               7034           2
__               7048           2
__               7057           2
__               7064           3
__               7069           2
__              10001           3
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Field	Description
Complex	The complex name for the security database.
useridTimestamp	The date and time to which the information pertains
Shared uids	The number of uids shared among multiple userids
OMVS uid	The z/OS UNIX uid
Occurrences	The number of RACF userids that share this uid

Select any of the uids for a list of the userids sharing the uid.

```
OMVS UIDs shared between RACF users                              Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR_
                                                  12 Sep 2000 00:07
   Complex  Timestamp  Shared uids
   TODAY    12Sep2000           14
            OMVS uid   Occurrences
                 5999           2
   Userid   OMVS uid   Name                 Owner    RIP SOA LastConDa LastPwdC
__ C##BVC1        5999 EPRISE VC USER       C##BVC           11Sep2000 04Sep199
__ C##BVC2        5999 EPRISE VC USER       C##BVC   YY
****************************** BOTTOM OF DATA ********************************
```

Field	Description
Userid	The RACF `userid`
OMVS uid	The z/OS UNIX uid (repeated to permit overtype in zSecure Admin).
Name	The user name
Owner	The owner of the user (profile)
RIP	The flags Revoked, Inactive, Protected (cannot logon).
SOA	The flags Special, Operations, Auditor (system authorities).
LastUseDa	The date of the user's last logon.
LastPwdCh	The date of the user's last password change.
LastPhrCh	The user's last password phrase change date.
InstData	Installation data field of the user profile.

The detail display shows the InstData field wrapped.

The SHRDGIDS and OMVSNGID reports are the equivalents of SHRDUIDS and OMVSNUID for groups and gids instead of users and uids. User-specific fields are, of course, not shown--just the InstData.

PWINLONG - Exceptional Password Interval reports

These reports show the user IDs that do not have to change their passwords often based on one of the following profile settings:

- An exceptionally long password interval.
- No password interval specified.
- Can logon without a password.
- Can logon with an OIDCARD.

You can also generate a report showing protected user IDs that do not have a password and cannot logon to the system.

You can generate the following types of reports:

PROTECT
Shows the protected users who have no password and cannot logon. These users are not listed in the other reports.

PWNONE
Shows users that have no password because they have another means of authentication.

PWOID
Shows the users who must supply an operator identification card when logging onto the system.

PWINNONE
Shows the users who never have to change their password because they have no password interval.

PWINLONG
Shows users that have an 'exceptionally long' interval. You can specify the threshold for this interval by editing the PWINLONG NEWLIST statements in the CARLa scripts `CKRDPWIN` and `CKRLPWIN`.

Also, when you configure these reports, you can exclude started task user IDs. If you follow IBM best practices and have configured your system with `list of groups checking` active, you can easily exclude these IDs using the special purpose group *STCGROUP* that the started task user IDs are connected to. You can do this by specifying *STCGROUP* in the select statements for the PWINLONG and PWINNONE NEWLISTs as shown in the following example for the PWINLONG report.

```
select class=user segment=base passint>60 passint<255,
     congrpnm<>stcgroup    /* exclude started tasks */
```

If you define more than 30 characters as *exceptionally long*, and your started tasks are connected to a special STRTASK group, you can customize this statement to specify these conditions as shown in the following example:

```
select class=user segment=base passint>30 passint<255,
     congrpnm<>strtask    /* exclude started tasks */
```

You can also modify the NEWLIST title.

All five reports have the same layout, containing a second-level summary categorizing the user IDs by revoked and inactive status. Inactive user IDs are those that are pending revoke because of a SETROPTS INACTIVE() setting. These IDs are revoked at the next logon attempt. The most interesting category are users that can logon–their access is not revoked or pending revoke.

Figure 219 shows a sample display for the PWINLONG report.

```
Users with password interval > 60 days                          Line 1 of 2
Command ===> ____________________________________________ Scroll===> CSR
                                              7 Mar 2001 00:07
   Complex  Timestamp  Users
   DINODAY   7May2001    380
   Revoke   Inactive   Users
   No       No             2
   Userid   Name                Int Eff LastPwdCh LastPhrCh DfltGrp  Owner
__ PWINUS1  LONG INTERVAL        90  90 28Apr2001           C#BEHEER SYSPROG
s_ PWINUS2  AUTHORIZED TOO       90  90 28Apr2001           C#BEHEER SYSPROG
```

Figure 219. PWINLONG report

The display contains the following fields of interest.

Field	Description
Complex	The complex name for the security database.
Timestamp	The date to which the information pertains.
Users	The number of users in the database.
Revoke	Whether the users in the category are revoked.
Inactive	Whether the users in the category are 'pending revoke', for example, if they tried to log on they would be revoked.
Users	The number of users in the category.
Userid	The userid.
Name	The user name.
Int	The password interval.
Eff	Effective password interval: the lowest of user and global interval.
LastPwdCh	The date of the user's last password change.

Field	Description
LastPhrCh	The user's last password phrase change date.
DfltGrp	The user's default group.
Owner	The owner of the userid.
RIRP	The flags Revoked, Inactive, Restricted, and Protected.
SOA	The flags Special, Operations, and Auditor.
gC	Shows whether the user has any group attributes or Clauth authority.
LCX	Shows whether the user has any RACLINKs, any certificates, or an expired password.
Try	The number of unsuccessful password attempts.

The detail display shows the groups the user is connected to, the user's last use date (which reflects both logons and certain updates), the date the user last logged on with any of the groups the user is currently connected to (this reflects the user's last logon date unless the connection to the group the user last logged on with was removed in the interim) [3] , the date the userid was defined, the last password change date, and the installation data.

```
Users with password interval > 60 days                          Line 1 of 9
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp  Users
   DINODAY   7May2001    380
   Revoke   Inactive   Users
   No       No            85
   Userid   Name                Int Eff LastPwdCh LastPhrCh DfltGrp  Owner
   PWINUS2  AUTHORIZED TOO       90  90 28Apr2001           C#BEHEER SYSPROG

  Group    Auth    R SOA AG Uacc    Revokedt    Resumedt
_ SYSPROG  USE             NONE

  User's last use date           2 Mar 2001 15:44
  Last RACINIT current connects  2 Mar 2001
  Creation date                 24 Dec 1998
  Password changed date         20 Mar 2001
  Installation data
****************************** BOTTOM OF DATA ********************************
```

PWEXPIRE - Expired Password report

This report shows the users that have an expired password.

The report has a second-level summary categorizing the userids according to their being revoked and/or inactive (for example, they are not yet revoked, but would be revoked because of the SETROPTS INACTIVE() setting when they next tried to logon) and/or their being unused. The most interesting categories would consist of those users that are able to logon, for example, those that are neither revoked nor pending revoke. Protected userids are excluded.

A sample display is shown in the following figure.

3. For the non-RDS, the last use date is shown here, too.

```
Users with expired passwords                                    Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp  Users
   DINODAY   7May2001    380
   Revoke   Inactive   Unused  Users
   No       No         No          2
   Userid   Name                Int Eff LastPwdCh LastPhrCh DfltGrp  Owner
__ BPXOINIT 01234567890123456890  50  50                     SYSAPPL  SYSAPPL
s_ C##BQAC4                       50  50                     C##BQA   C##BQA
```

The display contains the same fields as the Exceptional Password Interval reports. Likewise, the detail display shows the groups the user is connected to, the user's last use date, the date the user last logged on with any of the user's current connect groups, the date the `userid` was defined, the last password change date, and the installation data.

The PHEXPIRE report shows the users that have an expired password phrase. It contains the same fields as the PWEXPIRE report.

PWNOCHG - Initial Password report

This report shows the users that appear to have never changed their password. That is, users that have a blank `last password change date`. Protected `userids` are excluded.

The report has a second-level summary categorizing the `userids` according to four criteria:

Recent
Whether these `userids` were only recently created (within the last two weeks); for these `userids` it is probably justifiable that they have an initial password.

Revoked
Indicates if the user is revoked and unable to logon to change the password.

Inactive
Whether the user (although technically not revoked) would be revoked when he attempted to logon now due to the SETROPTS INACTIVE() setting. This does not happen if the `userid` has never been used–the Last use date is empty.

STCgroup
Whether the `userid` is a started task. In order for this indication to function correctly, you might need to customize the determination criterion in the CKRDPWNU and CKRLPWNU CARLa scripts utilized in this report. For example, fill in the correct connect group name (congrpnm) to recognize started tasks by in the where clause of the DEFINE STCGROUP statement (the default is STCGROUP). Also see the example in “PWINLONG - Exceptional Password Interval reports” on page 302.

A sample display is shown in Figure 220 on page 306.

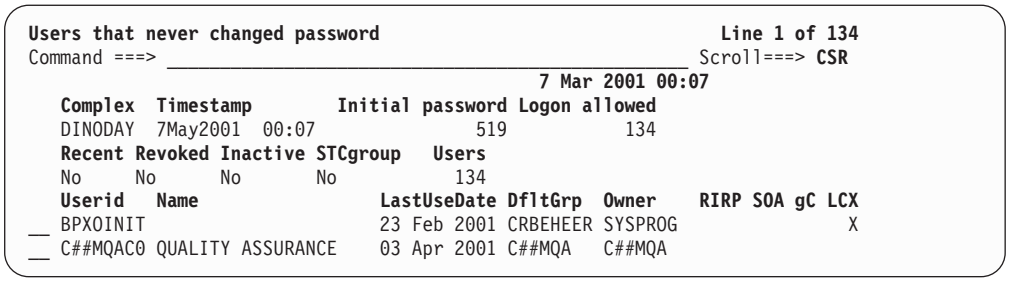


Figure 220. Users that never changed password panel

Table 170 provides the descriptions for the fields of interest on this panel.

Table 170. Users that never changed password - field descriptions

Field	Description
Complex	The complex name for the security database.
Timestamp	The date and time to which the information pertains.
Initial password	The number of users in the database that have an initial password.
Logon allowed	The number of users with an initial password that can successfully logged on. That is, the user ID is neither revoked nor inactive.
Recent	Whether the user IDs in the category were defined within the last two weeks.
Revoked	Whether the user IDs in the category are revoked.
Inactive	Indicates if the user IDs in the category are *pending revoke*. That is, if they tried to log on they would be revoked.
STCgroup	Whether the `userids` in the category are started tasks (if you properly customized the recognition criterion).
Users	The number of `userid` in the category.
Userid	The user ID.
Name	The user name.
LastUseDate	The date of the user's last logon.
DfltGrp	The user's default group.
Owner	The owner of the `userid`.
RIRP	The flags Revoked, Inactive, Restricted, and Protected.
SOA	The flags the Special, Operations, and Auditor attributes.
gC	Shows whether the user has any group attributes or Clauth authority.
LCX	Shows whether the user has any RACLINKs, any certificates, or an expired password.
Try	The number of unsuccessful password attempts

The detail display shows the groups the user is connected to, the user's last use date, the date the user last logged on with any of the user's current connect groups, the date the `userid` was defined, the last password change date, the last password phrase change date, and the installation data.

The PHNOCHG report shows the users that have never changed their password phrase. It contains the same fields as the PWNOCHG report.

PWAGE - Password and Password Phrase Age reports

The Password age overview report summarizes the following password data for all user IDs:

- Security database identification information and a summary of password information that includes the total number of user IDs, user IDs that still use the initial password, and user IDs with an active, non-revoked password.
- User IDs reported by password status: Non-revoked (active and available for log on), pending, or revoked.
- Number of user IDs with a password that has never changed.
- The Passwords listed by password age, which indicates the time elapsed since the last password change.

  The reports lists passwords age by year for passwords older than a year and by month for passwords that have changed within the past year.

Figure 221 shows the Password age overview report.

```
RACF password age overview
Command ===> _____________________________________________ Scroll===> CSR
                                                  26 Apr 2001 16:23
   Complex  Timestamp  Users Initial password Initial nonrevoked
   DINO     26Apr2001    671              519                134

__                    Non-revoked    Pending    Revoked  All users
   Number of userids:         188         73        410        671
   Never changed:             134         44        341        519

   Age in years:
   Older than 5 years:                                4          4
   4..5 years old:              5          2          8         15
   3..4 years old:              1          4         12         17
   2..3 years old:              2          8         15         25
   1..2 years old:              1         12         13         26
   0..1 years old:             45          3         17         65

   Specification of age 0..1 years:
   6..12 months old:            5          3         16         24
   5..6 months old:             5                     1          6
   4..5 months old:             2                                2
   3..4 months old:             2                                2
   2..3 months old:             2                                2
   1..2 months old:            14                               14
   2..4 weeks old:              2                                2
   0..2 weeks old:             13                               13
****************************** BOTTOM OF DATA ********************************
```

Figure 221. RACF password age overview

The combined Password and Password Phrase Age detail report uses the same dimensions. On the first level, which precedes the database selection level, you select the age interval of interest as shown in Figure 222 on page 308.

```
zSecure Audit Display Selection                    1 s elapsed, 0.8 s CPU
Command ===> ____________________________________________________ Scroll===> CSR

  Name     Summary Records Title

_ PWAGEALL       2    2582 User Password or Phrase Age: All users
_ PWAGENEV       2    1293 User Password or Phrase Age: Initial password
_ PWAGE5YR       2    1141 User Password or Phrase Age: 5 years or more
_ PWAGE4YR       1      15 User Password or Phrase Age: 4..5 years
_ PWAGE3YR       1      17 User Password or Phrase Age: 3..4 years
s PWAGE2YR       1      25 User Password or Phrase Age: 2..3 years
_ PWAGE1YR       1      26 User Password or Phrase Age: 1..2 years
_ PWAGE0YR       1      65 User Password or Phrase Age: Less than a year
_ PWAGE6MN       1      24 User Password or Phrase Age: 6..12 months
_ PWAGE5MN       1       6 User Password or Phrase Age: 5..6 months
_ PWAGE4MN       1       2 User Password or Phrase Age: 4..5 months
_ PWAGE3MN       1       2 User Password or Phrase Age: 3..4 months
_ PWAGE2MN       1       2 User Password or Phrase Age: 2..3 months
_ PWAGE1MN       1      14 User Password or Phrase Age: 1..2 months
_ PWAGE2WK       1       2 User Password or Phrase Age: 2..4 weeks
_ PWAGEREC       1      13 User Password or Phrase Age: Less than 2 weeks
****************************** Bottom of data ******************************
```

Figure 222. RACF Password age detail report

Next, you select the database to review, followed by the user category depending on the revoke and inactive status. The panel shown Figure 223 shows the detailed password information.

```
User Password or Phrase Age: 2..3 years                          Line 1 of 2
Command ===> ____________________________________________________ Scroll===> CSR
                                              5 Mar 1998 00:05
   Complex  Timestamp  Users
   DINO      5Mar1998      4
   Revoke   Inactive   Users
   Yes      Yes            2
   Userid   Name                LastPwdCh LastPhrCh DfltGrp  Owner    RI SOA T
__ C#MBURG  BURGH, RUDOLPH      06Feb1996           C#MB     C#MB     YY
__ IBMUSER  IBM DEFAULT USER    07Dec1995           SYS1     IBMUSER  YY   Y
****************************** BOTTOM OF DATA ******************************
```

Figure 223. RACF User Password or Phrase Age report

This display contains the following fields of interest.

Field	Description
Complex	The complex name, that is the database).
Timestamp	The date to which the information pertains.
Users	The number of users in the database with a password age in between two and three years.
Revoke	Whether the users in the category are revoked.
Inactive	Whether the users in the category are 'pending revoke', for example, if they tried to log on they would be revoked.
Users	The number of users in the category.
Userid	The user ID.
Name	The user name.
LastPwdCh	Date of the last password change.
LastPhrCh	The date of the last password phrase change.
DfltGrp	The user default group.

Field	Description
Owner	The owner of the user ID.
RI	Flags that indicate if the user ID status is *Revoke* or *Inactive*. or inactive.
SOA	The flags Special, Operations, and Auditor.
Try	The number of unsuccessful password attempts.

The detail display shows the groups the user is connected to, the user's last use date, the date he last logged on with any of his current connect groups, the date the `userid` was defined, the last password change date, the last password phrase change date, and the installation data.

Note: In print format, the equivalents of the `PWAGEALL` and `PWAGE0YR` fields are not supported. They contain information that is available in other entries so it is not necessary to include them in the report.

PWTRIES - Failed Logon Attempts report

This report shows the users that tried to logon with an invalid password and did not successfully complete a logon since. The second summary level shows the different counts of subsequent invalid password attempts, and the number of users for each count. (If you are only interested in this summary level, you can use the concise display).

A sample (detailed) display is shown in the following figure.

```
Users with logon failures                                          Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR
                                          7 Mar 2001 00:07
   Complex  Timestamp         Users
   DINODAY   7May2001  00:07      9
   PwTry    Users
       5        1
   Userid   Name                 LastUseDate DfltGrp  Owner    RIRP SOA Try
__ C##QA017                      18 Sep 1997 C##QA    C##QARUN YY         5
****************************** BOTTOM OF DATA ********************************
```

This display contains the following fields of interest.

Field	Description
Complex	The complex name (for example which database).
Timestamp	The date and time to which the information pertains.
Users	The number of users with logon failures.
PwTry	The number of failed attempts.
Users	The number of users with this number of failed attempts.
Userid	The `userid`.
Name	The user name.
LastUseDate	The date of the user's last logon.
DfltGrp	The user's default group.
Owner	The owner of the `userid`.
RIRP	The flags Revoked, Inactive, Restricted (user has no access via GAC, UACC, and ID(*)), and Protected (user cannot logon).

Field	Description
SOA	The flags Special, Operations, Auditor (user has system authority).
Try	The number of unsuccessful password attempts.

The detail display shows the groups the user is connected to, the user's last use date, the date he last logged on with any of his current connect groups, the `userid`'s definition date, the last password change date, the last password phrase change date, and the installation data.

LGNEVER - Never Used Userids reports

This report shows the users that appear to have never been used (that is, userids that have an uninitialized last use time). One thing to keep in mind is that `userids` that have never been used are not subject to SETROPTS INACTIVE() processing, when the userids have been created on a system older than z/OS 1.7.

The report has a second-level summary categorizing the user IDs based on the following criteria:

Recent
Whether these user IDs have been created within the last two weeks. For recently created user IDs, it is probably justifiable to not yet have been used.

Revoked
Whether the `userid` is revoked, and therefore cannot be used at present.

Inactive
Whether the user (although technically not revoked) would be revoked when the user attempted to logon now due to the SETROPTS INACTIVE() setting. (=No)

Protected
Whether the user is protected (that is, does not have a password and cannot logon).

STCgroup
Whether the `userid` is a started task. In order for this indication to function correctly, you might need to customize the determination criterion in the CKRDLGNU and CKRLLGNU CARLa scripts utilized in this report. To customize the criterion fill in the correct connect group name (`congrpnm`) to recognize started tasks in the where clause of the DEFINE STCGROUP statement (the default is STCGROUP). See also the example in "PWINLONG - Exceptional Password Interval reports" on page 302.

A sample display is shown in Figure 224 on page 311.

```
Users that have never been used                                    Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR
                                              7 Mar 2001 00:07
   Complex  Timestamp        Never used Logon allowed
   DINODAY   7May2001  00:07        449           123
   Recent Revoked Inactive Protected STCgroup Users
   No     No      No       Yes       No          21
   Userid   Name                LastPwd LastPhr DfltGrp  Owner    RIRP SOA TRY
__ LDAPSRV  LDAP server                          SYS1     SYS1        Y
****************************** BOTTOM OF DATA ********************************
```

Figure 224. User IDs that have never been used report

The display panel contains the following fields of interest.

Field	Description
Complex	The complex name (for example which database).
Timestamp	The date and time to which the information pertains.
Never used	The number of users in the database that have never been used.
Logon allowed	The number of users that have never been used that can successfully logon. That is, the user ID is neither revoked nor inactive.
Recent	Indicates if the user IDs in the category were defined within the last two weeks.
Revoked	Indicates if the user IDs in the category are revoked.
Inactive	Indicates if the user IDs in the category are *pending revoke*. That is, the password for the user ID is revoked at the next logon attempt.
Protected	Indicates if the user IDs in the category are protected.
STCgroup	Indicates if the user IDs in the category are started tasks. This value is reported (if you properly customized the recognition criterion).
Users	The number of user IDs in the category.
Userid	The user IDs.
Name	The user name.
LastPwd	The date of the last password change for the user ID.
LastPhr	The last password phrase change date for the user ID.
DfltGrp	The default group for the user.
Owner	The owner of the user ID.
RIRP	Flag fields that indicate the password status: • **R**evoked • **I**nactive • **R**estricted (user has no access through `GAC`, `UACC`, and `ID(*)`. • **P**rotected (user cannot logon).
SOA	Flag fields indicating the following special authority: • Special • Operations • Auditor (user has system authority)
Try	The number of unsuccessful password attempts.

Select a user ID entry in the report to view the following detailed password and password phrase nformation:

- Groups the user is connected to.
- Last use date.
- Date last logged on with any of the current connect groups.
- User ID definition date.
- Last password change date.
- Last password phrase change date.
- Installation date.

LGREVOKE - Inactive Userids report

These reports show which systems take measures to revoke users that have not logged on for too many days, and for those that do, which users would be revoked due to inactivity if they tried to logon.

LGNOREV - Systems that do not revoke users due to inactivity

The systems listed specify SETROPTS NOINACTIVE and thus take no measurements against `userids` that are no longer used. There are no further details available.

A sample display is shown in the following figure.

```
Systems that do not revoke users due to inactivity              Line 1 of 1
Command ===>                                                  Scroll===> CSR
                                            29 Aug 1994 08:55
   Complex  System   Collect time stamp
   MVS510   ML1E     29 Aug 1994 08:55
****************************** BOTTOM OF DATA ********************************
```

LGREVOKE - Users pending revoke because of inactivity

This report shows which users would be revoked due to inactivity if they tried to logon.

A sample display is shown in the following figure.

```
Users pending revoke because of inactivity                    Line 1 of 76
Command ===> ____________________________________________________ Scroll===> CSR
                                            7 Mar 2001 00:07
   Complex  Timestamp        Users
   DINODAY   7May2001  00:07    76
   Userid   Name                 LastConDate DfltGrp  Owner    RIRP SOA Try
__ AOP      AOP SYSTEM DATA                  ZY#APPL  ZY#APPL   Y         0
__ BPXOINIT                                  ZY#APPL  ZY#APPL   Y         0
__ C##BDMW  DAVID WISSER         26 Mar 1998 C##B     C##B      Y         0
```

The display contains the following fields of interest.

Field	Description
Complex	The complex name (for example which database).
Timestamp	The date to which the information pertains.
Users	The number of users in the database that are pending revoke.
Userid	The `userid`.

Field	Description
Name	The user name.
LastConDate	Estimate of the user's last logon date; for the RDS, the maximum of the RACINIT dates for the user's connect groups; for the non-RDS, the user's last use date.
DfltGrp	The user's default group.
Owner	The owner of the `userid`.
RIRP	The flags Revoked, Inactive, Restricted (user has no access via GAC, UACC, and ID(*)), and Protected (user cannot logon).
SOA	The flags Special, Operations, Auditor (user has system authority).
Try	The number of unsuccessful password attempts

The detail display shows the groups the user is connected to, the user's last use date, the date the user last logged on with any of the user's *current* connect groups, the date the `userid` was defined, the last password change date, the last password phrase change date, and the installation data.

LGAGE - Last Logon Date reports

The Last Logon Summary report summarizes the user population according to the length of time the users have not logged on, and the revoke and pending revoke statuses. The Last Logon Details report shows the user population similarly broken into categories.

For the RDS we use the date of the last logon with any of a user's current connect groups as the best estimate of the last logon date; note that if the connection to the group the user last logged on with is removed in the interim, this cannot be accurate. For the non-RDS use the LJDATE to capture all logon events. The LJDATE is also updated with certain updates. If you want to revert to the prior practice of using the LJDATE for the RDS too, you can edit the following CARLa script members. Change LAST_CONNECT_DATE into LJDATE except where it occurs as `last_connect_date(detail,prefix)` in the detailed display in addition to LJDATE

- CKRDLGAG (summary display)
- CKRLLGAG (summary list)
- CKRDLGAD (detailed display)
- CKRLLGAD (detailed list)
-

Figure 225 on page 314 shows a sample summary.

```
RACF last logon overview                                          Line 1 of 1
Command ===> _____________________________________________ Scroll===> CSR
                                                  26 Apr 2001 16:23
   Complex  Timestamp  Users Never logged on Unused nonrevoked
   DINO     26Apr2001    711             559               151

__                   Non-revoked    Pending    Revoked  All users
   Number of userids:         211         76        424        711
   Never logged on:           151         36        372        559

   Last logon in years ago:
   More than 5 years:                                2          2
   4..5 years:                                 2     13         15
   3..4 years:                                 8     11         19
   2..3 years:                                 7      6         13
   1..2 years:                                11      5         16
   0..1 years:                    60          12     15         87

   Specification of last logon 0..1 year ago:
   6..12 months:                   1          12     14         27
   5..6 months:                    3                             3
   4..5 months:                    6                 1           7
   3..4 months:                    1                             1
   2..3 months:                    6                             6
   1..2 months:                    4                             4
   2..4 weeks:                     3                             3
   0..2 weeks:                    36                            36
****************************** BOTTOM OF DATA ********************************
```

Figure 225. RACF last logon overview panel

The summary line at the top shows the complex name (which database) with time stamp, the number of users in the database, how many of them have never yet logged on, and how many of those could now successfully logon, for example, they are neither revoked nor inactive.

The section that follows shows the number of userids that are either active or inactive, followed by the total number of userids. The next row shows the number of userids that have never logged in.

The last sections show the number of userids that did log on broken down per year. The last year is broken down further.

The Last Logon Date Details report uses the same dimension, plus the protected attribute. On the first level (which even precedes the database selection level), you select the time interval you are interested in as shown in the following figure.

```
zSecure Audit Display Selection                  Line 1 of 16
Command ===> _____________________________________________ Scroll===> CSR

   Name     Summary Records Title
_ LGAGEALL       2    2622 User Last Logon: All users
_ LGAGENEV       2    1039 User Last Logon: Never logged on
_ LGAGE5YR       2    1433 User Last Logon: 5 years or more ago
_ LGAGE4YR       1      15 User Last Logon: 4..5 years ago
_ LGAGE3YR       1      19 User Last Logon: 3..4 years ago
s LGAGE2YR       1       4 User Last Logon: 2..3 years ago
_ LGAGE1YR       1      16 User Last Logon: 1..2 years ago
_ LGAGE0YR       1      87 User Last Logon: Less than a year
_ LGAGE6MN       1      27 User Last Logon: 6..12 months ago
_ LGAGE5MN       1       3 User Last Logon: 5..6 months ago
_ LGAGE4MN       1       7 User Last Logon: 4..5 months ago
_ LGAGE3MN       1       1 User Last Logon: 3..4 months ago
_ LGAGE2MN       1       6 User Last Logon: 2..3 months ago
_ LGAGE1MN       1       4 User Last Logon: 1..2 months ago
_ LGAGE2WK       1       3 User Last Logon: 2..4 weeks ago
_ LGAGEREC       1      36 User Last Logon: Less than 2 weeks
****************************** Bottom of data ********************************
```

Figure 226. Display Selection screen

Next, you select the database to review, and then the user category depending on the revoke, inactive, and protected statuses. This leads to a user display as shown in the following figure.

```
 User Last Logon: 2..3 years ago                                Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
                                                  5 Mar 1998 00:05
    Complex  Timestamp  Users
    DINO      5Mar1998      4
    Revoke   Inactive   Protected  Users
    Yes      Yes        No         2
    Userid   Name                LastConDate DfltGrp  Owner    RIP SOA Try
__  C#MBURG  BURGH, RUDOLPH       6 Feb 1996 C#MB     C#MB     YY        0
__  P#90     REVOKED USER        16 Feb 1996 P#90M5   SYSPROG  YY        0
****************************** BOTTOM OF DATA ********************************
```

Figure 227. User Display screen

This display contains the following fields of interest.

Field	Description
Complex	The complex name (for example which database).
Timestamp	The date to which the information pertains.
Users	The number of users in the database with a password age in between two and three years.
useridRevoke	Whether the users in the category are revoked.
Inactive	Whether the userids in the category are pending revoke, for example, if they tried to log on they would be revoked.
Protected	Whether the userids in the category are protected.
Users	The number of users in the category.
Userid	The userid.
Name	The user name.
LastConDate	Estimate of the user's last logon date; for the RDS, the maximum of the RACINIT dates for the user's connect groups; for the non-RDS, the user's last use date.
DfltGrp	The user's default group.

Field	Description
Owner	The owner of the `userid`.
RIP	The flags Revoked, Inactive, and Protected (user cannot logon).
SOA	The flags Special, Operations, Auditor (user has system authority).
Try	The number of unsuccessful password attempts.

The detail display shows the groups the user is connected to, the user's last use date, the date the user last logged on with any of the user's current connect groups, the date the `userid` was defined, the last password change date, the last password phrase change date, and the installation data.

Note: In the print format, the equivalents of the LGAGEALL and LGAGE0YR fields are not present in the report because this information is already included in other fields in the report and would be redundant in the printed report.

STATUS AUDIT - RACF resource

This section describes RACF reports on the protection of resources (for example, data sets), resource profile audit concerns, and database resource usage (for example, size). The reports that include data sets require a full CKFREEZE read.

More RACF reports are available in the CARLa library or from the main menu options **RA** and **AU.V**. You are advised to run the collection batch report `CKRL$ALL`, which includes other reports, at least once.

The following RACF reports are described in this section:

- RACPRAUD - RACF Resource Profile Audit Concerns report
- SENSTRUS - Sensitive Data Trustees report
- SENSPROF - Sensitive Data by Profile report
- ENTITY - Entity and segment summaries
- APFPROT - Authorized Programs reports
- PADS - Program Access to Data Sets report
- STCPROT - Started Task protection report
- GLBW - Globally writable data reports
- UIDNOUSR - UNIX ids used in the file system, but not defined to RACF

RACPRAUD - RACF Resource Profile Audit Concerns report

This report shows audit concerns for general resource profiles. A sample display is shown in the following figure.

```
RACF profile audit concerns                                    Line 1 of 63
Command ===> ____________________________________________ Scroll===> CSR
                                          5 Mar 1998 00:05
   Complex  Timestamp       Audit concerns Priority
   DINO      5Mar1998  00:05             63       10
   Pri Class    Profile key                              Audit concern
__ 10 DATASET  CATALOG.UCAT.**                          Verify why UACC>=U
__ 10 DATASET  ONEQUAL.**                               Verify why UACC>=U
__ 10 DATASET  ONEQUAL.SMPMCS                           Verify why UACC>=U
__ 10 DATASET  SYS1.BRODCAST                            Verify why UACC>=U
__ 10 DATASET  USERCAT.**                               Verify why UACC>=U
__ 10 FACILITY $CNG.CMD.CMD.ASK.*                       Verify why UACC>=U
__ 10 FACILITY $CNG.USRDATA.OWN.USER.PHONE              Verify why UACC>=U
__ 10 NODES    &C#MNODE.RUSER.*                         Verify why UACC>=U
__ 10 SDSF     ISFATTR.OUTPUT.*                         Verify why UACC>=U
__  6 APPCSERV NON.GENERIC.AST*                         Generic chars in d
s_  3 VMPOSIX  LOOKS.LIKE.GENERIC.*                     Profile not used f
```

The display contains the following fields of interest.

Field	Description
Complex	The complex name
Timestamp	The date and time to which the information pertains.
Audit concerns	The number of profiles for which audit concerns were found.
Priority	The highest audit priority found for any profile.
Pri	The audit priority.
Class	The profile class.
Profile key	The profile key.
Audit concern	Any audit concerns identified. This value might be truncated.

On the detail display, the profile's installation data is shown, as well as all audit concerns in their entirety.

```
RACF profile audit concerns                                    Line 1 of 4
Command ===> ____________________________________________ Scroll===> CSR
                                          5 Mar 1998 00:05
   Complex  Timestamp       Audit concerns Priority
   DINO      5Mar1998  00:05             63       10
   Pri Class    Profile key                              Audit concern
     3 VMPOSIX  LOOKS.LIKE.GENERIC.*                     Profile not used f
  InstData

  Audit concern
  Profile not used for access control, Class inactive, Generic chars in
  discrete key
****************************** BOTTOM OF DATA ******************************
```

The audit concerns that can occur are documented in “RACF: RACF profiles” on page 1124.

SENSTRUS - Sensitive Data Trustees report

A common audit function is to review who can compromise sensitive resources. For some data sets like the RACF database, APF data sets, and page/swap data sets, updates must be tightly controlled. For other data sets, , read access to the information must be tightly controlled. In zSecure, sensitive resources are those that can be accessed and used directly or indirectly to bypass normal system

security. Trusted users are those that have access to these sensitive resources. If a hacker wants to bypass the normal security controls, it is sufficient for him or her to guess, sniff, or steal the password of any of the trusted user IDs.

You can use the Sensitive Data Trustees report to audit sensitive resources and review the user access to these resources. The information reports the user access, grouped by sensitive resource type. To see similar information grouped by user, see the "TRUSTUSR - Trusted users report" on page 292.

Auditing sensitive data

You can customize the Sensitive data trustees report to audit JES2 procedure libraries used for batch jobs that are considered sensitive by checking the **JES2 JOB proclibs considered sensitive** option on the customization panel of the STATUS AUDIT menu. You can achieve the same effect in a batch job by including the CARLa command SIMULATE SENSITIVE PROCLIB.

Figure 228 shows a sample of the Sensitive data trustees report.

```
Sensitive data trustees                                          Line 1 of 30
Command ===> _____________________________________________ Scroll===> CSR
                                                  15 Sep 2000 00:07
   Pri Complex  System   Trust relations
    10 TODAY    DINO              3822
   Pri Sensitivity Class    Resources Trust relations
__  10 Privilege   System           1              28
__  10 Surrogate   SURROGAT        11              58
s_  10 TrustedFile FSOBJ            6              28
__  10 TrustedHome FSOBJ            3              20
__   9 APF library DATASET         47             275
__   9 APF Linklst DATASET         38             229
__   9 APF LPAlist DATASET          2              12
__   9 MSTR prmlib DATASET          3              20
__   9 MSTR STClib DATASET          3              18
__   9 Resource    FACILITY        16             136
__   9 RACF prim   DATASET          1             417
__   9 STC joblib  DATASET          1               8
__   9 STC proclib DATASET          7              42
__   8 Resource    TSOAUTH          2              17
__   7 JES2 Ckpt   DATASET          2             106
__   5 HFS dataset DATASET         86             635
__   5 JES2 prmlib DATASET          1               6
__   5 JES2 Spool  DATASET          1              12
__   5 Pagedataset DATASET          6              36
__   4 RACF back   DATASET          1             393
__   4 RMM Control DATASET          1               7
__   4 RRSFdataset DATASET         22             308
__   4 System Dump DATASET          3              27
__   4 SMF dataset DATASET          3             909
__   3 HSM BCDS    DATASET          1               7
__   3 HSM MCDS    DATASET          1               7
__   3 HSM OCDS    DATASET          1               7
__   2 SMS ACDS    DATASET          1              18
__   2 SMS COMMDS  DATASET          1              18
__   2 SMS SCDS    DATASET          1              18
****************************** BOTTOM OF DATA ********************************
```

Figure 228. Sensitive data trustees report - Summary information

Table 171 describes the fields of interest on the summary panel.

Table 171. Sensitive data trustees report - Summary information field descriptions

Field	Description
Pri	The highest audit priority for any audit concern for the system.
Complex	The complex name.

Table 171. Sensitive data trustees report - Summary information field descriptions (continued)

Field	Description
System	The system name.
Trust relations	The number of audit concerns identified.
Pri	The highest audit priority for this sensitivity type.
Sensitivity	The sensitivity type, used to group similar resources.
Class	The resource class used by z/OS to secure the resource.
Resources	The number of resources of the same sensitivity type.
Trust relations	The number of ways a user can exploit the sensitivity type.

To view details about the sensitive resources for a specific sensitivity type, enter / in the entry field for that sensitivity type. Figure 229 shows the detail view for the `TrustedHome FSOBJ` sensitivity type.

```
Sensitive data trustees                                          Line 1 of 6
Command ===> ____________________________________________ Scroll===> CSR
                                          15 Sep 2000 00:07
   Pri Complex  System   Trust relations
    10 TODAY    DINO               3822
   Pri Sensitivity Class    Resources Trust relations
    10 TrustedFile FSOBJ            6              28
   Pri Resource                                    VolSer Trust relations
__  10 /.profileRoot                                                    6
s_  10 /u/automount/r##slin/.profileRoot                                1
__   9 /u/automount/c##bert/.profile                                    1
__   3 /.sh_history                                                    18
__   3 /u/automount/c##bert/.sh_history                                 1
__   3 /u/automount/r##slin/.sh_history                                 1
****************************** BOTTOM OF DATA ********************************
```

Figure 229. Sensitive data trustees report - Detail information

Table 172 describes the fields of interest on the detail panel.

Table 172. Sensitive data trustees report - field descriptions for detailed view for resource type

Field	Description
Pri	The highest audit priority for this resource.
Resource	The name of the resource.
Volser	The volume serial if the resource is a data set.
Trust relations	The number of ways a user can exploit the resource.

To see the users that have access to any resource and the type of access each user has, type a / in the entry field next to the resource name to open the User access view panel shown in Figure 230 on page 320.

```
Sensitive data trustees                                          Line 1 of 1
Command ===> ____________________________________________ Scroll===> CSR_
                                          5 Feb 2004 17:10
   Pri Complex  System   Trust relations
    10 TODAY    DINO               3822
   Pri Sensitivity Class    Resources Trust relations
    10 TrustedFile FSOBJ            6              28
   Pri Resource                                  VolSer Trust relations
    10 /u/automount/r##slin/.profileRoot                              1
   Pri Userid   Name                 From     Audit concern
    10 C##BERT  ERIC TWAIN           TODAY    Can use Trojan attacks via the .p
   Pri Privilege Via      Access  Profile
s_  10 UnixOwner          UPDATE
****************************** BOTTOM OF DATA ********************************
```

Figure 230. Sensitive data trustees report - User access view

Table 173 lists the fields of interest in the Sensitive data trustees report.

Table 173. Sensitive data trustees report - field descriptions for user access view

Field	Description
Pri	The highest audit priority for this user/resource pair.
Userid	A user with sufficient authorization to compromise the resource.
Name	The name of the user.
From	The complex from where the user can compromise the resource.
Audit concern	An explanation of the risk.
Pri	The audit priority for this user/resource/profile triple.
Privilege	The kind of authorization instrumental for the access.
Via	The group id that grants the user access (when access is given via a group.)
Access	The access level granted to the user on the 'From' complex.
Profile	The profile key in the 'From' complex covering the resource.

The detail display panel shown in Figure 231 on page 321 reports the user access information in the following categories: object at risk, the rule that grants the sensitive access, and the subject (user ID) that is trusted.

```
Sensitive data trustees
Command ===> _____________________________________________ Scroll===> CSR_
                                          5 Feb 2004 17:10


  Sensitive object
  Complex that may be attacked  TODAY
_ System that may be attacked   DINO
  Type of sensitive resource    TrustedFile
  Resource class                FSOBJ
_ Resource name                 /u/automount/r##slin/.profileRoot
  Volume serial for resource
  Access level that is exposure WRIT-NX

  Security rule covering object
  Complex used for the attack   TODAY
  RACF profile class
  RACF profile

  User that may compromise security
_ Trusted userid                C##BERT  ERIC TWAIN
  Revoked (may be by date)
  Inactive, revoked or pending
  Password disabled   PROTECTED
  Privilege on user's complex   UnixOwner
  Id associated with privilege
  Access level granted to user  UPDATE
  Relative audit priority       10
  Audit concern                 Can use Trojan attacks via the .profile of
  Audit concern                 trusted user R##SLIN
****************************** BOTTOM OF DATA ********************************
```

Figure 231. Sensitive data trustees report - field descriptions for user access view

This example shows user *C##BERT*, who is trusted because he can update the `.profile` of trusted user *R##SLIN* because he is the file owner. `.profile` is a script executed when a user logs on to the z/OS UNIX system. The full UNIX path name of the `.profile` is shown in Figure 231 and any write access is considered sensitive as indicated by the value *WRIT-NX*.

SENSPROF - Sensitive Data by Profile report

A common audit function is to verify that sensitive data sets are adequately protected. For some data sets (like APF data sets, security databases, and page/swap data sets), updates must be tightly controlled. For other data sets (security database, page/swap data sets), read access to the information must be tightly controlled. zSecure Collect recognizes some sensitive data sets automatically, and Security zSecure verifies RACF protection according to either *confidentiality* or *integrity* demands. The automatically checked sensitive data sets are:

- APF data sets (integrity)
- LPA data sets (integrity)
- Page data sets (confidentiality and integrity)
- Swap data sets (confidentiality and integrity)
- RACF data sets (confidentiality and integrity)
- RRSF data sets (confidentiality and integrity)
- SMF recording data sets (confidentiality and integrity)
- System dump data set (confidentiality and integrity)
- TSO user administration data set UADS (confidentiality and integrity)
- Other system data sets: SYS1.NUCLEUS and SYS1.LPALIB (integrity).
- JES2 and JES3 checkpoint data sets (confidentiality and integrity)

- JES2 and JES3 spool data sets (confidentiality and integrity)
- JES2 and JES3 parameter data set (confidentiality and integrity)
- JES2 and JES3 STC/TSU proclib (integrity)
- MSTR proclib (integrity)
- MSTR parameter library (integrity)
- MSTR VIO administration (integrity)
- DFHSM data set BCDS, MCDS, OCDS (integrity)
- HFS data sets (integrity)
- DMS database DMSFILES (integrity)
- DMS authorized parameter library (integrity)
- DMS default parameter library (integrity)
- CA1 tape management catalog TMC (integrity)
- DFSMS SCDS and ACDS (integrity)
- IODF file, if DSN could be found (integrity)
- Couple data sets (integrity)
- RMM control dataset (integrity)
- TLMS volume master file VMF (integrity)
- ABR archive control file ACF (integrity)

You can audit the sensitive data set protection by generating the Sensitive Data by Profile report which shows the sensitive data sets and their protection, organized by covering profile.

Notes:

1. This report does not treat all systems equally, so be careful not to select multiple input sets on different systems.
2. The intended report to simply look at sensitive data sets in an MVS system without particular regard to their protection is the Sensitive Data Sets report in the MVS EXTENDED category. See “SENSITIVE - Sensitive Data Set report” on page 518.

Background

You can add your own data sets by means of the SIMULATE SENSITIVE command. For more information, see “SIMULATE” on page 911. LINKLIST data sets are automatically reported as APF data sets, unless the IEASYS*xx* member in your system contains LNKAUTH=APFLST. If LINKLIST data sets are not automatically APF authorized, you can use the SIMULATE SENSITIVE LINKLIST command to report LINKLIST anyhow. SIMULATE SENSITIVE PROCLIB can be used to flag integrity problems in the JES2 proclibs used for batch jobs.

Auditing Sensitive Data

When ensuring that all sensitive data sets are adequately protected and audited, a particular audit concern is that the APF list is up to date. If a library contained in the APF list or an authorized library in the LNKLST concatenation does not actually exist on the system, users can create their own data set and then rename it to have the name of the missing APF library, thus creating their own authorized programs. Missing data sets are marked as *notfnd* in the report.

The information included in the sensitive data report can be customized using the following options:

System
Specify a system to be used for primary point of view.

All datasets
Show all data sets that are covered by the profiles that cover any sensitive data sets.

Linklist sensitive
Consider all LNKLST concatenation data sets to be sensitive, for example, even if the LNKLST concatenation is not authorized.

Proclib sensitive
Consider all JES2/JES3 JOB proclibs to be sensitive.

When using the STATUS AUDIT menu, you can simply specify the desired options in the customization panel.

When generating this report with a batch job, you can specify the desired options with CARLa commands included with the standard scripts as listed in the following table.

Table 174. Sensitive data set report - CARLa commands for batch reporting

Information to include in report	CARLa statement
System	DEFAULT SYSTEM= *smf_id*
All data sets	REPORT DATASETS
Linklist sensitive	SIMULATE SENSITIVE LINKLIST
Proclib sensitive	SIMULATE SENSITIVE PROCLIB

In addition, you can also identify additional sensitive data sets to be included with the SIMULATE SENSITIVE command. For details, see "SIMULATE" on page 911. When using the STATUS AUDIT menu, you can put these additional commands in your preamble using the primary command "SETUP 3".

Figure 232 shows the display panel with the Profiles covering sensitive data sets report.

```
Profiles covering sensitive data sets                          Line 1 of 144
Command ===> _____________________________________________ Scroll===> CSR
                                                 7 Mar 2001 00:07
   Complex  Timestamp         Profiles Audit concerns Priority
   DINO     7 Mar 2001 00:07      144              2       10
   Pri Profile key                                  UACC    Era S/F Audit conce
__  10 CATALOG.**                                   READ    NO    R No alter au
__  10 CRMBMR2.**                                   NONE    NO    R No update a
__     ASM.SASMMOD1                                 READ    NO  U R
__     ASM.SASMMOD2                                 READ    NO  U R
__     ASM.SASMSAM1                                 READ    NO  U R
```

Figure 232. Profiles covering sensitive data sets

The display contains the following fields of interest.

Field	Description
Complex	The complex name of the system used as the primary viewpoint.
Timestamp	The date and time the information pertains to.
Profiles	The number of profiles and High-level qualifiers reported.

Field	Description
Audit concerns	The number of profiles and High-level qualifiers for which audit concerns were found.
Priority	The highest audit priority found for any profile or High-level qualifier.
Pri	The audit priority for the profile or High-level qualifier.
Profile key	The profile key, or the High-level qualifier if no covering profile was found.
UACC	The universal access level.
Era	Whether erase-on-scratch is active for the profile.
S/F	The lowest access level that results in auditing for successes and failures, respectively. The values for the success access level and the failure access level are separated by a blank.
Audit concern	Audit concerns identified.

A detail display is shown in the following table.

```
Profiles covering sensitive data sets                          Line 1 of 18
Command ===> _____________________________________________ Scroll===> CSR
                                                 7 Mar 2001 00:07
  Type    Sensitivity Volume Profile key / data set name
  GENERIC                    CATALOG.**
   clustr              n/a   CATALOG.ETP.EXIC
    data              ETPSMS CATALOG.ETP.EXIC
    index             ETPSMS CATALOG.ETP.EXIC.CATINDEX

  User/grp Access  WhenProg
_ SYSAUTH  OWNER
_ ASM      QUALOWN
_ SYSPROG  ALTER

  Profile attributes
  Security complex name         DINODAY
  Universal access authority    READ
  Erase-on-scratch              NO
  Audit access success/failures   R

  Audit concern
  Relative audit priority       10
  Audit concern                 No alter audit
****************************** BOTTOM OF DATA ******************************
```

The detail display shows the following extra fields.

Table 175. Profiles covering sensitive data sets - detail display field descriptions.

Field	Description
Type	For a data set, either the resource type (see the first table below) or 'notfnd' for a missing APF library; for a profile, the profile type, or (for a High-level qualifier) 'missing' if no profile was found.
Sensitivity	Indication why this data set is considered sensitive.
Volume	The volume serial of the data set
Profile key/ data set name	The profile key (or HLQ) followed by the sensitive data sets covered
Access list	The access list of the profile
Audit concern	Any identified audit concerns (see the second table below)

The resource types that can be shown are listed in the following table.

Table 176. Profiles covering sensitive data sets - resource types

nvsam	Non-VSAM disk data set, migrated if volume is MIGRAT (for HSM or ABR), or archived if the volume is ARCIVE (for DMS). This information is obtained from the VTOC for data sets on disk, the HSM MCDS and the ABR ACF for migrated data sets, and the DMSFILES data set for archived data sets. The information is not derived from the catalog entries.
clustr	VSAM cluster (catalog entry). The volume listed is the volume of the catalog. The source for the cluster names can be a catalog, HSM MCDS, ABR ACF, DMS DMSFILES data set, or VVDS.
bkpclu	Backup of a VSAM cluster. Normally, this is only listed below a backed-up discrete profile such as a discrete profile with a system-generated name. The source for the cluster name is the HSM BCDS or a DMS DMSFILES data set.
index	Index component of a VSAM cluster residing on the indicated DASD volume.
data	Data component of a VSAM cluster residing on the indicated DASD volume.
aixix	Index component of a VSAM alternate index residing on the indicated DASD volume.
aixda	Data component of a VSAM alternate index residing on the indicated DASD volume.
migcl	Migrated or archived VSAM cluster. This is listed below a cluster entry instead of the components. The volume is equal to MIGRAT or ARCIVE.
clust	Backup of VSAM cluster. This is listed below a `bkpclu` entry instead of the components. The volume is equal to MIGRAT or ARCIVE.
gdg	Base name of a GDG (Generation Data Group), obtained from a catalog.
cnntap	Cataloged, unmanaged tape file, on an unmanaged volume.
unntap	Uncataloged, non-managed tape file, on a non-managed volume. The source for such an entry is probably the TVTOC of a TAPEVOL profile.
cmmtap	Cataloged, managed tape file on a managed, non-scratch tape volume.
ummtap	Uncataloged, managed tape file on a managed, non-scratch tape volume.

Table 176. Profiles covering sensitive data sets - resource types (continued)

cnmtap	Cataloged, unmanaged file on a managed, non-scratch volume. This means that the catalog entry conflicts with the tape management information.
unmtap	Uncataloged, non-managed file on a managed, non-scratch volume. The source for such an entry is probably the TVTOC of a TAPEVOL profile.
cnstap	Cataloged, non-managed file, on a managed volume in scratch status.
unstap	Uncataloged, non-managed file, on a managed volume in scratch status. The source for such an entry is probably the TVTOC of a TAPEVOL profile.
secvol	Secondary volume of a multi-volume data set.

The audit concerns that can be identified are shown in the following table.

No erase	Erase on scratch required for confidentiality
No read audit	Read audit required for confidentiality
No update audit	Update audit required for integrity
No alter audit	Alter audit required for integrity
Read fail audit	Read failure audit required for confidentiality
Update fail audit	Update failure audit required for integrity
Alter fail audit	Alter failure audit required for integrity
UACC too high	Universal access should be NONE or READ
Warning mode access	Warning mode on profile resulted in ALTER access
Global access	The access given through the Global Access Table is too high
Unprotected	There is no profile protecting the data set, and PROTECTALL(FAILURES) is not set
ID(*) too high	ID(*) on the access list has too high access

ENTITY - Entity and segment summaries

STATUS AUDIT option ENTITY displays reports that show the number of segments defined and the amount of space used, summarized by entity type and segment.

The ENTITY#S report summarizes by entity type, which means that all GENERAL classes are grouped together. Figure 233 provides an example of the overview display panel.

```
Entity segment summary by descending number of bytes              Line 1 of 4
Command ===>                                                   Scroll===> CSR
                                              12 Sep 2002 11:03
   Complex  Timestamp
   ZOS14TMP 12Sep2002  11:03
   TotalBytes Entity   Segments
__      288913 GENERAL      1465
s_      214345 USER         1064
__      176103 DATASET       825
__       46062 GROUP         428
****************************** BOTTOM OF DATA ********************************
```

Figure 233. Entity segment summary by descending number of bytes - display panel

Any entity type can be selected to display the segment types defined for the entity type.

```
Entity segment summary by descending number of bytes              Line 1 of 16
Command ===> _____________________________________________________ Scroll===> CSR
                                                  12 Sep 2002 11:03
   Complex  Timestamp
   ZOS14TMP 12Sep2002  11:03
   TotalBytes Entity   Segments
       214345 USER         1064
   TotalBytes Segment  Segments
__     182165 BASE          544
__      13923 TSO           132
__       5765 OMVS          154
__       2605 PROXY          20
__       2184 NETVIEW        46
__       2035 DCE            33
__       1186 OPERPARM       21
__        771 LNOTES         22
__        678 NDS            20
__        665 WORKATTR       12
__        645 CICS           16
__        611 KERB            7
__        392 DFP            14
__        363 OVM            11
__        252 LANGUAGE        9
__        105 EIM             3
****************************** BOTTOM OF DATA ********************************
```

Figure 234. Entity segment summary by descending number of bytes - display panel

The SEGMENT report summarizes by the segment types defined.

```
Class segment summary by descending number of bytes               Line 1 of 22
Command ===> _____________________________________________________ Scroll===> CSR
                                                  12 Sep 2003 11:03
   Complex  Timestamp
   ZOS14TMP 12Sep2002  11:03
   TotalBytes Segment  Segments
__     591230 BASE         2818
__      85760 CERTDATA       89
__      13923 TSO           132
__       7375 OMVS          231
__       7228 STDATA        162
__       3164 PROXY          24
__       2981 TME             6
__       2184 NETVIEW        46
__       2035 DCE            33
__       1878 DFP            73
__       1186 OPERPARM       21
__        996 KERB           12
__        771 LNOTES         22
s_        758 EIM            17
__        680 SESSION        12
__        679 SIGVER          8
__        678 NDS            20
__        665 WORKATTR       12
__        645 CICS           16
__        407 OVM            13
__        331 SSIGNON         7
__        252 LANGUAGE        9
__        196 SVFMR           4
__        100 DLFDATA         3
****************************** BOTTOM OF DATA ********************************
```

Figure 235. Entity defined segment type report - display panel

Any segment type can be selected to display the classes having profiles that include the segment type.

```
Class segment summary by descending number of bytes         Line 1 of 2
Command ===>                                                  Scroll===> CSR
                                              12 Sep 2002 11:03
   Complex  Timestamp
   ZOS14TMP 12Sep2002  11:03
   TotalBytes Segment  Segments
          758 EIM            17
   TotalBytes Class    Segments
          566 LDAPBIND       13
          105 USER            3
           87 FACILITY        1
***************************** BOTTOM OF DATA ********************************
```

Figure 236. Entity segment type profile classes report - display panel

APFPROT - Authorized Programs reports

The authorized program reports show the protection of load modules that have the potential to circumvent RACF. This report includes the following information:

- AC(1) members of all APF libraries with all their entry points.
- Modules in APF libraries that are present in the Program Property Table (PPT) with the BYPASS option or a system key (0-7).
- Modules in APF libraries that are present in the RACF authorized caller table with RACINIT or RACLIST authorization.

For z/OS UNIX, the files that run with APF authorization are shown, as well as program-controlled files, and files that run under the file owner identity rather than the identity of the user running them (SETUID/SETGID).

Background

The TSOAUTH, LPAPROT, and APFPROT reports include the highest access to arbitrary users as given by the combined action of the PROGRAM profile UACC, the DATASET profile UACC, the LNKLST concatenation residency, the LPA residency, the global access table, and the profile warning mode. In addition, the report shows all module occurrences with LNKLST concatenation and LPA list concatenation numbers, the MLPA residency in-storage, the base member names for alias entries, the authorizing attributes, the attributes extending the authorization to the TSO environment (AuthCMD AuthPGM AuthTSF), and the RACF profile member names.

Note: These reports do not treat all systems equally, so be careful about multiple input sets.

You can specify a minimum universal access level of interest for entries to be included in these reports, as well as the system to be used as the primary viewpoint for these reports. If you use the STATUS AUDIT menu, you are automatically prompted with a customization panel to select reporting options for the access level and the SMF id for the primary system. In a batch run, these options are set with the CARLa commands REPORT ACCESS= level or DEFAULT SYSTEM=*smf_id*, respectively.

The meaningful access levels that can be specified are shown in the following table.

Table 177. APFPROT - UACC levels and descriptions

Level	Meaning
ALTER	ALTER access.
CONTROL	CONTROL access.
UPDATE	UPDATE access.
READ	READ access.
READLPA	The UACC does not grant READ access, but the module can be read in the LPA.
LOADEXE	The UACC does not grant READ access, but the module can be executed and read using LOAD.
EXECUTE	Execute access.
COPY	A module can be read, but not executed. If the operation does not depend on APF or library residence, then anyone can access its functionality by copying it to his or her own load library.
HIDDEN	A PDS member or load module hidden by a similarly named member in a library in front of this library.

The UNIXAPF, UNIXCTL, UNIXSUID, and UNIXSGID reports show the z/OS UNIX files that run with the following attributes: APF authorized, program-controlled, SETUID and SETGID, respectively.

APF authorization attribute
Files with the extended attribute *a* run APF authorized. The FACILITY resource BPX.FILEATTR.APF setting determines who can enable the APF authorization.

Program-controlled attribute
Files with the BPX.FILEATTR.PROGCTL protects the *p* extended attribute (program control). Together with UPDATE access to one of the FACILTY profiles BPX.DAEMON or BPX.SERVER, a controlled environment permits process or thread identity switches.

If BPX.DAEMON has `READ` access and `UID=0`, identity switches with the `spawn` and `SETUID` attributes are permitted.

`SETUID` and `SETGID` attribute
The `SETUID` and `SETGID` attributes basically mean that a program runs under the identity of the file owner (`UID` or `GID`) instead of the current user. `UID=0` implies UNIX superuser authority. Only a superuser can set these attributes. When a file is copied, these bits are turned off. When a file is moved, they are kept. When a file is written to, the extended attributes are removed; for setuid and setgid to be kept, the same authority is required as for turning them on in the first place.

Notes:

1. Strictly speaking, these UNIX reports show directory entries rather than files. In UNIX, the same file can have several path names known as hard links. The actual file is identified by an *inode* number, which is basically an index number within the Hierarchical File System. If there are several hard links to a file, the Authorized Programs report shows multiple directory entries for the file. Security is regulated at the inode level, but the effective file attributes also depend on the path name (hard link). Although a file can only be accessed with sufficient authority over the directories in its path, it is generally not prudent to rely on the security of a specific path being inaccessible, because of this link concept.

2. The CKFREEZE file used for these reports must include PDS directory information as well as UNIX file system information. This means that zSecure Collect must be run with the FOCUS=AUDITACF2 or FOCUS=AUDIT setting and UNIX=YES, preferably APF authorized (for completeness). If zSecure Collect is run unauthorized, you must specify PDS=YES and make sure that the program has sufficient access to all LNKLST concatenation and APF data sets. The UNIX ACL information is only available if zSecure Collect is run with UNIXACL=YES as well.

Auditing Authorized Programs

In a safe system, the security policy regarding the use of utilities that have the potential to bypass MVS, RACF, ACF2, or TSS protection mechanisms must be one of protection-by-default. Before permitting universal access to such utilities, you must perform a risk analysis.

In an MVS system, it can prove surprisingly difficult to determine the exact protection of AC=1 APF modules. For example, it is not uncommon that more than one module with the same name is available in the system. In addition, a number of questions must be answered to get a complete picture of the protection including the following:

1. Do the DATASET profiles covering the APF data sets containing the module have the attribute setting UACC(NONE) attribute.
2. Is the module covered by a PROGRAM profile in all data sets?
3. Does the PROGRAM profile have the attribute setting UACC(NONE)?
4. Is one of the APF data sets part of the LNKLST concatenation?
5. Which APF or non-APF authorized data set is the first in the LNKLST concatenation to contain the module?
6. Is the module present in the LPA?
7. Is the module present in the MLPA?
8. Is the data set covered by a global access table entry with an access level of READ or higher?
9. Is the data set profile in warning mode?

The TSOAUTH and LPAPROT reports have the same layout as the APFPROT report shown in Figure 237 on page 331 but exclusively show the TSO-authorized commands and LPA modules instead of all APF-authorized programs.

Figure 237 on page 331 shows a sample of the ISPF display panel for the Authorized programs report.

```
APF module protection overview                                  Line 1 of 595
Command ===>                                                  Scroll===> CSR_
                                                    6 Mar 1998 00:05
   Complex  System   Timestamp         Count
   DINO     DINO      6 Mar 1998 00:05   595
   Module   UACC     AuthAttr Member   Datasetname
__ @CKGRACF NONE     AC=1     @CKGRACF C#MA.D.CNRMCO.SC2RLOAD
__ @NFCOLL  NONE     AC=1     @NFCOLL  C#MA.T.CNR221.SC2RLOAD
__ @NFCOLL  NONE     AC=1     @NFCOLL  C#MA.T.CNR221.PR70809.SC2RLOAD
__ @RSPEC   NONE     AC=1     @RSPEC   C#MBGUS.FRUT.LOAD
__ AHLGTF   NONE     Key 0    AHLGTF     *** no module found ***
__ AKPCSIEP NONE     Key 1    AKPCSIEP   *** no module found ***
s_ ALTER    READ     <more>   IDCAM01  SYS1.CMDLIB
__ AMASPZAP READ     AC=1     AMASPZAP SYS1.MIGLIB
__ ANTDFRR  READ     AC=1     ANTSDMLE SYS1.LPALIB
__ ANTDIO   READ     AC=1     ANTSDMLE SYS1.LPALIB
```

Figure 237. APF module protection overview panel

Table 178 lists the fields of interest for the APF module protection overview panel.

Table 178. APF module protection overview - field descriptions

Field	Description
Complex	The complex name for the security database.
System	The system name.
Timestamp	The date and time the information pertains to.
Count	The number of (entry points in) APF-authorized modules
Module	The name of an entry point in the module.
UACC	The consolidated universal access to the module, taking into account `PROGRAM` profile `UACC`, `DATASET` profile `UACC`, global access table, `LNKLST` concatenation residency, `LPA` residency, and warning mode. The UACC field can have the following values: *READLPA*. The data set `UACC` does not permit read access, but the module can be read in LPA. *LOADEXE*. The data set `UACC` does not permit read access, but the module can be run and read with the `LOAD` command. Running the `LOAD` command requires that you know the module name. *HIDDEN*. The module `UACC` is `NONE` because it is hidden by a module with the same name, concatenated in front of the `LPA` or `LNKLST` concatenation. *COPY*. The module can be read but not run. If its operation does not depend on APF authorization or library residence (`PADS`), all users can access its functionality by copying it to their own load library.

AuthAttr	The source of authorization for the module, which can be any of the following values: *AC=1*. Indicates permission to issue a `MODESET` command. *Bypass*. Bypass RACF and password security, from Program Property Table (PPT). *Key=n*. Alternate key (not key 8), from Program Property Table (PPT). *RACINIT*. RACINIT authority, from RACF authorized caller table ICHAUTAB. *RACLIST*. RACLIST authority, from RACF authorized caller table ICHAUTAB. *PADS*. Present on a conditional access list. *AuthPGM*. Can be called under TSO as an authorized program. *AuthCMD*. Can be called as TSO authorized command. *AuthTSF*. Can be called as authorized through the TSO service facility. *IEAAPP00*. I/O appendage authorized for use by non-APF users. **Note:** If the module has several sources of authorization, the `AuthAttr` column on the overview display panel only shows the first one. The list of authorization sources can be found on the detail display or by scrolling to the far right.

Member	PDS member name. This value differs from the module name in case the module has an alias name.
Datasetname	Contains the name of the data set containing the member. **** LPA **** indicates that the module was in the LPA but could not be found in any of the PDS directories. This value can also mean that the in-storage AC=1 attribute for the data set is different. **** module not found **** indicates that the module was not found in LPA or in any PDS (partitioned data set), but would have had special authorizations if present.
Volume	Volume serial containing the data set in the previous column.
x**LPA**	Identifies the LPA type: *P* for `PLPA`, *M* for `MLPA`, or *F* for `FLPA`. In addition, the sequence number in the LPA list concatenation of the data set is displayed.
h	Indicates that the module is hidden–not accessible through the `LPA` list or `LNKLST`. If applicable, this value (*h*) is listed between the **LPA** and **Lnk** columns.
Lnk	Contains the sequence number of the data set in the `LNKLST` concatenation. If the data set is not part of the `LNKLST` concatenation, the field is blank.
PROGRAM	This column contains the name of the program profile covering the module (if any).
PType	Indicates the mode of Program Control (z/OS V1R4 and up). Either blank, BASIC, or MAIN.

DATASET profile	Contains the name of the data set profile covering the data set. The value can be truncated if your line length is less than 153. In addition to the data set profile, this column can also include an entry from the global access table. The following columns are derived from the `AuthAttr` field: *AC1*. Can issue the `MODESET` command. *Byp*. Bypass RACF and password security, from `PPT`. *Key*. Alternate key (not key 8), from Program Property Table PPT. *Ini*. RACINIT authority–from the RACF authorized caller table ICHAUTAB. *Lst*. RACLIST authority–from the RACF authorized caller table `ICHAUTAB`. *PAD*. Present on a conditional access list. *PGM*. Can be started under TSO as an authorized program. *CMD*. Can be called as a TSO authorized command. *TSF*. Can be called as authorized through the TSO service facility. *APP* I/O appendage authorized for use by non-APF users.

You can select any module for a detail display by entering the **S** action character. To browse a module from the list, type the **B** action character in the entry field.

Tip: For an overview of the available actions, type the / action character in front of the module name.

```
APF module protection overview (except UNIX files)              Line 1 of 22
Command ===> _____________________________________________ Scroll===> CSR_
                                          7 Mar 2001 00:07


  Load module identification
  Program module name           ADDGROUP
  Library member name           IRRENV00
_ Data set name                 SYS1.LINKLIB
  Volume serial                 R8RES1

  Authority and resulting protection
  Authorization attributes      AC=1 AuthCMD
  Consolidated universal access LOADEXE

  Contributing system properties
  System name                   DINO
  Linklist concat number        1
  Member hidden in linklist     NO
  LPA list concat number
  MLPA or FLPA

  Contributing RACF properties
  Security complex name         DINODAY
  PROGRAM profile               *
  Program type
  DATASET profile               SYS1.LINKLIB
****************************** BOTTOM OF DATA ********************************
```

Figure 238. Detail display of a module

When looking at UNIX files, the first thing to pay attention to is the file mode, which determines the access to the file in conjunction with the Access Control List (ACL). The file mode consists of three groups of access controls for the owning UID, for the owning GID, and for users that do not have an owning ID.

Each group is shown in three positions. The first position represents read access, the second write access, the third execute access. The third position can show the following additional user or group ID information:

- *s* or *S* for `setuid` (in the first group)
- *t* or *T* for the sticky bit property (in the third group).

A lowercase *s* or *t* indicates that the execute bit is on. The uppercase value indicates that execute bit is off.

For the files in these reports, make sure to inspect the global execute access, which is indicated by an *x* or *t* in the last position of the `FileMode` field. Also check the files to determine whether they have the correct privileges to begin with. You can examine other concerns, such as the protection of the file system where the files are stored, through the “SENSTRUS - Sensitive Data Trustees report” on page 317.

Note: If the UNIXPRIV class is active and RACLISTed, and the RESTRICTED.FILESYS.ACCESS resource is protected by a profile in that class, then RESTRICTED users are not granted access on the basis of the third ("other") group, unless they have a least READ access to the RESTRICTED.FILESYS.ACCESS resource.

The UNIX ACL contains the access permissions for additional users and groups, including *. The owning UID access bits take precedence over user entries on the ACL, which take precedence over any group entries. The owning GID and additional group entries on the ACL have the same precedence, and access given by any of them is granted. Only if none of these apply, the third ("other") group is checked.

A sample UNIXAPF display is shown in the following figure.

```
UNIX files with APF authorization                                  Line 1 of 7
Command ===> ____________________________________________________ Scroll===> CSR_
                                                    14 Sep 2000 00:07
   Pri Complex   System   APF files
    11 TODAY     DINO           88
   Pri APF files FS mount point
__  11         4 /u/automount/c##8090
__  11        15 /u/automount/c2rnew
s_  11         4 /u/automount/c2rsrv#p
__  11         2 /u/automount/CNR250
__  11         2 /u/automount/C2RSRV#P
__  11         1 /u/automount/PR91241
__   8        60 /
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Field	Description
Pri	The highest audit priority for any audit concern for the system.
Complex	The complex name which identifies the security database.
System	The system name
APF files	The total number of APF authorized files in the file system
Pri	The highest audit priority for any audit concern for a mount point.
APF files	The number of APF authorized files in the mounted file system.
FS mount point	The directory at which the file system is mounted.

Select any mount point for a list of files with APF authorization.

```
UNIX files with APF authorization                                  Line 1 of 4
Command ===> ____________________________________________________ Scroll===> CSR_
                                                    14 Sep 2000 00:07
   Pri Complex   System   APF files
    11 TODAY     DINO           88
   Pri APF files FS mount point
    11         4 /u/automount/c2rsrv#p
   Pri T FileMode  + apsl AuF Owner    Group    Relative pathname (within FS)
__  11 - rwxr-x---   aps  fff C2RINST  C##QA    checkpass
__  11 - r-xr-x---   aps  fff C2RINST  C##QA    c2rserve/bin/bbracf
s_  11 - r-xr-x--- + aps  fff C2RINST  C##QA    c2rserve.1.1.1999mar17/c2rserve/b
__  11 - rwxr-x---   aps  fff C2RINST  C##QA    c2rserve.1.1.5/bin/bbracf
****************************** BOTTOM OF DATA ********************************
```

Field	Description
Pri	The audit priority for this file

Field	Description
T	The type of file: regular file (-), block special file (b), character special file (c), directory (d), external symlink (e), symlink (l), pipe or FIFO (p), socket (s).
FileMode	The effective file mode, shown as lists of permissions for specific groups. The groups are owner (u), group (g), and other (o). When the permissions of all groups are equal, an (a) is used. The permissions can be read (r), write (w), execute (x), setuid/setgid (s), and sticky bit (t). The setuid/setgid and sticky bits indicators are shown in uppercase (S/T) when execute permission is off. Note that this format is the same as used by the chmod command.
+	Whether this file has any of the following extended ACL entries: access, directory default, or file default.
apsl	The effective extended attributes, shown as a list of attributes that are on (+) and a list of attributes that are off (-). Possible attributes are APF authorization (a), program controlled (p), address space sharing (s), and library sharing (l).
AuF	The combined audit flags: three positions for read, write, and execute access, each specifying **s** for successes, **f** for failures, **a** for all, or **-** for none. "Combined" means that either the owner or an auditor has requested auditing.
Owner	The RACF `userid` that is mapped to the owning uid. If there are several such RACF userids, this is the alphabetically first one.
Group	The RACF group that is mapped to the owning gid. If there are several such RACF groups, this is the alphabetically first one.
Relative pathname (within FS)	Path name relative to the file system's mount point.

Select any file for a detail display. You can browse the regular files in the displayed list by entering the **b** action character.

```
UNIX files with APF authorization                              Line 1 of 45
Command ===> _____________________________________________ Scroll===> CSR_
                                          14 Sep 2000 00:07

  System view of file
  Complex name                  TODAY
  Sysplex name                  LOCAL
  System name                   DINO
_ Absolute pathname             /u/automount/c2rsrv#p/c2rserve.1.1.1999mar17/c2
_ Absolute pathname             rserve/bin/bbracf
  FS mounted with SECURITY      Yes
  FS mounted with SETUID        Yes
  FS mounted READ/WRITE         Yes
  File access attributes        o=,ug=rx
  Security label
  Extended file attributes      +aps
  Effective audit flags         =f
_ Owner name                    C2RINST C2RSRV#P PTKTCHK
_ Group name                    C##QA
  Device                        1891
  Relative audit priority       11
  Audit concern                 executable file runs APF-authorized (extattr
  Audit concern                 +a), executable file runs program-controlled
  Audit concern                 (extattr +p)

  Physical file attributes
  Complex that owns file system TODAY
  System that owns file system  DINO
  File system data set name     C##BOMVS.U.C2RSRV#P.HFS
  Volume serial for file system SM3003
  File system DASD serial + id  IBM-51-000000068569-0802
  Relative pathname within FS   c2rserve.1.1.1999mar17/c2rserve/bin/bbracf
  File type                     -
  Physical access attributes    o=,ug=rx
  Physical extended attributes  +aps
  User-requested audit flags    =f
  Auditor-specified audit flags =
  User id                       10001
  Group id                      9000
  Inode number                  150
  File audit id                 01E2D4F3F0F0F833F4090000048E0000
  Number of hard links          1

 User     TOrwx ACL id   UID/GID    Name                 InstData
 -group-   gr-x C##QA    9000                         CRM Q.A. TESTSUBJECT
 C2RINST   ur-x C2RINST  10001      C/RACF WIN INSTALLER C/RACFWIN INSTALL USERI
 C2RSRV#P  ur-x C2RSRV#P 10001      Zsecur ADMIN WINDOWS C/RACF WIN SERVER PROD
 C2RTEST   +r-x C2RTEST  1313       Zsecur TEST          ACL SUPPORT
 PTKTCHK   ur-x PTKTCHK  10001      CHECK PASSTICKET     RACTRACE AUTO ACTIVATED
 - any -   o--- -other-  n/a
****************************** BOTTOM OF DATA *******************************
```

Figure 239. UNIX files with APF authorization

The display is divided into three sections. The first section shows the effective settings. For example, the absolute pathname consists of the relative pathname within the HFS or zFS data set, prefixed by the mount point of the file system. The effective flags take the mount attributes and mode into account. The second section shows the physical characteristics, such as the flags actually indicated in the file system itself. The third section shows the UNIX access lists. An access ACL can be shown for any file type. For a directory, a directory default and a file default ACL can be shown as well.

By entering the action character **B** in front of the ABSOLUTE PATHNAME in the displayed panel, it is possible to browse the contents of the file.

The system view contains the following fields.

Table 179. UNIX file detail display - System view of file fields

Field	Description
Complex name	The complex name for the security database
Sysplex name	The sysplex name.
System name	The system name.
Absolute pathname	The full path name for the file.
FS mounted with SECURITY	Whether the file system is mounted with the SECURITY attribute. If not, any user can access and change any file in it.
FS mounted with SETUID	Whether the file system is mounted with the `SETUID` attribute. The following attributes are only honored if this attribute is set: setuid, setgid, APF, and program control attributes.
FS mounted READ/WRITE	The mode in which the file system is mounted. The mode can be either of the following values: • *READ* The file system is mounted read-only. • *RDWR* The file system is mounted with read and write access.
File access attributes	The effective file mode, shown as lists of permissions for specific groups. The groups are shown using the following values: *u* for owner, *g* for group, *o* for other, or *a* or all. The permissions can be *r* read, *w* write, *e* execute, *s* setuid or setgid, and for sticky bit setuid is indicated by the value *u*; setgid is indicated by the value *g*.
Security label	The file security label.
Extended file attributes	The effective extended attribute. The + symbol indicates an active attribute; the - symbol indicates an inactive attribute.
Effective audit flags	The effective audit flags. Flags are listed as successes (*s*) and failures (*f*) for each of the following access types: *r* read, *w* write, and *e* execute. If the access type does not matter, the flags are listed in a single list.
Owner name	The RACF `userid` that maps to the file uid. If there are more such users, a list is shown.
Group name	The RACF group that maps to the file gid. If there are more such groups, a list is shown.
Device	The device number identifying the mount point.
Relative audit priority	The audit priority for this file.
Audit concern	The audit concerns identified for this file. The audit concerns that can be identified can be found in "UNIX: UNIX System Services File System" on page 1480.

The display contains the following physical file attributes.

Table 180. UNIX file detail display - Physical file attributes fields

Field	Description
Complex that owns file system	Complex of the system that owns the file system.
System that owns file system	System that owns the file system.
File system data set name	The name of the data set that holds the file system.

Table 180. UNIX file detail display - Physical file attributes fields (continued)

Field	Description
Volume serial for file system	The volume serial of the HFS or zFS data set.
File system DASD serial + id	Manufacturer/Factory/Serial identifying the DASD, and device tag id (port) assigned to this volume on the owning system.
Relative pathname within FS	Path name relative to the file system's mount point.
File type	Indicates the UNIX file type which can have any of the following values: • - regular file • *p* pipe (or FIFO) • *d* directory • *b* block special file • *e*external symlink • *s*socket • *c* character special file • *l* symlink.
Physical access attributes	The physical file mode, shown as lists of permissions for specific groups. The groups are shown as *u* for owner, *g* for group, *o* for other, or *a* or all. The permissions can be *r* read, *w* write, *e* execute, *s* setuid or setgid, and sticky bit (setuid is indicated by the value *u*; setgid is indicated by the value *g*).
Physical extended attributes	The physical extended attributes, shown as a list of attributes that are on (+) followed by a list of attributes that are off (-).
User-requested audit flags	The audit flags requested by the owner, shown as lists of Flags are listed as successes (*s*) and failures (*f*) for each of the following access types: *r* read, *w* write, and *e* execute. If the access type does not matter, the flags are listed in a single list.
Auditor-specified audit flags	The audit flags specified by the auditor, shown similarly.
User id	The user ID for the file.
Group id	The group ID for the file.
Inode number	The inode number which identifies the file within the file system.
File audit id	The ID for the auditor.
Number of hard links	The number of directory entries for the file. A UNIX file has no canonical path name. The inode identifies a file within the file system. File attributes and other information is associated with the inode, not the path name.

The UNIX access control list contains the following fields.

Table 181. UNIX file detail display - Access control list fields

Field	Description
User	The user ID to which the entry pertains. This field can also contain the following values: • *-group-* shows up for an unexpanded ACL or an exploded ACL for an empty group when the **ACL id** field shows the group. • *-undef-* indicates that the user ID or group ID in an unexpanded or exploded ACL does not correspond to an existing RACF ID. • *-any-* indicates a global access setting.
TOrwx	The ACL Type. The value can be any of the following: • ACL type: *d* directory default, *f* file default, blank for access. • ACL entry Origin: *u* owning user, *g* owning group, *o* other, + ACL entry, or *a* Auditor attribute. • Access permissions indicate if the ID has authority to read (*r*), write (*w*), or execute (*x*).
ACL id	A RACF user or group associated with the UID/GID. This column can show a RACF user or group, or any of the following special origin values: • *-group-* for an owning group GID. • *-other-* for the global access setting. • *-any-* indicates any user. • *-owner-* for a file owner UID. • *-ACLuid-* for a UID on the ACL. • *-ACLgid-* for a GID on the ACL. • *-audit-* for directory read/execute access through the system-wide AUDITOR attribute. • *-more-* when an actual access level has more than one origin.

Table 181. UNIX file detail display - Access control list fields (continued)

Field	Description
UID/GID	The UID or GID that grants this access, or an indication why none applies. This value represents a UID if the value is a number, a RACF identity was determined, and the ACL ID contains either *-owner-* or *-ACLuid-*. Otherwise, the value represents a GID. This column can also contain the following special values: • *n/a* for the global access setting. • *-any-* for the user owner. • *-more-* for a composite entry or when read, write, and execute access to a directory is granted to a user on the basis of the RACF auditor attribute. For an exploded ACL, this field can have one of the following values: • *-no uid-* when there is no associated UID, either directly or through the BPX.DEFAULT.USER. • *-no gid-* when there is no associated GID.
Name	The user name.
InstData	The installation data for the user or group.

The layout of the UNIXCTL report on program controlled files is identical to that of the UNIXAPF report. The UNIXSUID and UNIXSGID report are the same as well, except that they have a few extra summary levels. Figure 240 shows a sample of the UNIXSUID report.

```
UNIX files with SETUID authorization
Command ===> _____________________________________________ Scroll===> CSR_
                                                 14 Sep 2000 00:07
   Pri Complex  System   Setuid files
     8 TODAY    DINO             106
   Pri Running under uid Setuid files
     4               110            1
   Pri Setuid files FS mount point
     4             1 /
   Pri T FileMode  + apsl AuF Owner    Group    Relative pathname (within FS)
__   4 - rwSr----x   --s  fff C##BERT           suidNOT0
****************************** BOTTOM OF DATA ********************************
```

Figure 240. UNIX files with SETUID authorization

The display contains the following fields of interest.

Field	Description
Pri	The highest audit priority for any audit concern for the system.
Complex	The complex name for the security database.
System	The system name.
Setuid files	The number of setuid files in the system.

Field	Description
Pri	The highest priority for files that switch to this identity.
Running under uid	The identity the file switches to.
Setuid files	The number of files that run under this identity.
Pri	The highest audit priority for any audit concern for a mount point.
Setuid files	The number of setuid files in the file system.
FS mount point	The directory at which the file system is mounted.
Pri	The audit priority for this file.
T	The file type.
FileMode	The effective file mode.
+	Indicates if this file has any of the following types of extended ACL entries: access, directory default, or file default.
apsl	The effective extended attributes.
AuF	The combined audit flags.
Owner	The RACF user ID that is mapped to the owning UID. If there are several such RACF `userids`, this is the alphabetically first one.
Group	The RACF group that is mapped to the owning GID. If there are several such RACF groups, this is the alphabetically first one.
Relative pathname (within FS)	Path name relative to the file system's mount point.

PADS - Program Access to Data Sets report

The display shows the protection of load modules that can be used for Program Access to Data Sets (PADS). These load modules are covered by program profiles present on the conditional access list of a DATASET profile. Usually, they give more access to the data set than the normal access list would grant.

Background

The report includes the highest access to arbitrary users as given by the combined action of PROGRAM profile UACC, DATASET profile UACC, LNKLST concatenation residency, LPA residency, global access table, and profile warning mode. In addition it shows all module occurrences with LNKLST concatenation and LPA list concatenation numbers, MLPA residency in-storage, base member names for alias entries, the authorizing attributes, attributes extending the authorization to the TSO environment (AuthCMD AuthPGM AuthTSF), and the RACF profile member names.

A CKFREEZE file is required. It must include PDS directory information for this function. This means that zSecure Collect must either be run APF-authorized with FOCUS=RACF or non-APF authorized with FOCUS=RACF,PDS=YES and sufficient access on all LNKLST concatenation and APF data set directories.

Note: This report does not treat all systems equally, so be careful about multiple input sets.

You can specify a minimum universal access level of interest for entries to be included in the report, as well as the system to be used as the primary viewpoint for the reports. If you use the ISPF STATUS AUDIT menu, you are automatically prompted with a customization panel where you can fill in the desired access level and SMF id of the desired primary system. In a batch run, include the CARLa commands REPORT ACCESS=level or DEFAULT SYSTEM=smf_id, respectively.

The meaningful access levels that can be specified are shown in the following table.

Level	Meaning
ALTER	ALTER access.
CONTROL	CONTROL access.
UPDATE	UPDATE access.
READ	READ access.
READLPA	The UACC does not permit READ access, but the module can be read in the LPA.
LOADEXE	The UACC does not permit READ access, but the module can be executed and read using LOAD.
EXECUTE	Execute access.
COPY	A module can be read, but not executed. If the operation does not depend on APF or library residence, then anyone can access its functionality by copying it to his or her own load library.
HIDDEN	A PDS member or load module hidden by a similarly named member in a library in front of this library.

Auditing Program Access to Data Sets

In a safe system, the security policy regarding the use of utilities that have the potential to grant special access to data sets must be one of protection-by-default. Update authority to libraries with such utilities must be tightly controlled. Universal access to these utilities must only be granted after performing a risk analysis.

In an MVS system, it can prove surprisingly difficult to determine the exact protection of program modules. For instance, it is not uncommon that more than one module with the same name is available in the system. In addition, a number of questions need to be answered to get a full picture of the protection for modules. These questions are:

1. Do the DATASET profiles covering the APF data sets containing the module have UACC(NONE) ?
2. Is the module covered by a PROGRAM profile in all data sets?
3. Does the PROGRAM profile have UACC(NONE)?
4. Is one of the APF data sets part of the LNKLST concatenation?
5. Which (APF or non-APF) data set is the first in the LNKLST concatenation to contain the module?
6. Is the module present in LPA?
7. Is the module present in MLPA?

8. Is the data set covered by a global access table entry with READ or higher?
9. Is the data set profile in warning mode?

The layout of the report is identical to that of the APFPROT report which is described in "APFPROT - Authorized Programs reports" on page 328.

STCPROT - Started Task protection report

This report shows the authority and protection defined for started tasks. The report combines information from the following sources:

- Started Procedure Table ICHRIN03
- RACF database
- JES2/JES3 proclib library concatenation in use for started tasks
- Procedure library used by the master address space (MSTR subsystem)

Note: If you are interested in the STARTED class and the Started Procedure Table rather than the protection of the started tasks, look at the STCTABLE report in "STCTABLE - Started Procedure Table and Started Class" on page 288.

Background

Started tasks are called by means of the START operator command, optionally with a SUB= parameter to indicate a target subsystem. The default subsystem is the primary subsystem, usually JES2 or JES3. Security zSecure supports both JES2 and JES3 as the primary subsystem, and in addition it supports the MSTR subsystem that is present in every MVS system.

It is important to curb access to the STC proclibs, because the JCL for started tasks with system authorization can be added or modified, and activated with a MVS START command without knowing the password of the authorized user.

Depending on the PTF level and RACF database level, a started procedure that is revoked might still run. However, it runs with reduced with reduced functionality which can result in problems submitting batch jobs, allocating new SMS-managed data sets, or obtaining printed output.

The consistency between ICHRIN03, the RACF database, and the JES2/JES3 proclibs can be verified with VERIFY STC (see "Finding inconsistencies in started task definitions" on page 367).

A `CKFREEZE` file is required to generate the report. The file must have been created with an authorized run of zSecure Collect. If you use `CKFREEZE` data collected during an unauthorized run with FOCUS=RACF,PDS=YES, this function only reports on the MSTR proclib without including information about the JES procedure libraries.

Note: This report does not treat all systems equally, so be careful about multiple input sets.

You can specify a different sort order, a minimum universal access level to select the entries to be included in the report, as well as system to be used as the primary viewpoint for the reports. In addition, you can exclude entries for undefined started task user IDs.

If you use the STATUS AUDIT menu, you are automatically prompted with a customization panel where you can specify these options. You can also customize and create the report in a batch process by using the CARLa commands listed in Table 182.

Table 182. Started Task protection report - CARLa command statements for generating the report

Reporting option	CARLa
Select a default system	DEFAULT SYSTEM=smf_id
Sort by member	REPORT BY=MEMBER
Exclude undefined userids	SUPPRESS ID=* ID=++++++++
Specify minimum UACC	REPORT ACCESS=level

You can specify any of the access levels listed in Table 183.

Table 183. Valid Access Levels for customizing the Started Task protection report

Level	Meaning
ALTER	ALTER access.
CONTROL	CONTROL access.
UPDATE	UPDATE access.
READ	READ access.
READLPA	The `UACC` does not grant `READ` access, but the module can be read in the LPA.
LOADEXE	The `UACC` does not permit `READ` access, but the module can be executed and read using LOAD.
EXECUTE	Execute access.
COPY	A module can be read, but not executed. If the operation does not depend on APF or library residence, then anyone can access its functionality by copying it to his or her own load library.
HIDDEN	A PDS member or load module hidden by a similarly named member in a library in front of this library.

Auditing Started Task Protection

Figure 241 on page 346 shows the overview panel for the Started Task Protection report.

```
Started task overview                                          Line 92 of 168
Command ===> _____________________________________________ Scroll===> CSR_
                                                  10 Sep 2002 14:33
   Complex  System   Timestamp         Count
   DINO     DINO     10 Sep 2002 14:33   168
   Procname Userid   Flags    Group    Subs Lib h Last updt By       STARTED pr
__ XWTR2    *              3           MSTR   1   01Feb1990 R##EY
__ ADM@SRV  ADM@SRV       DSu KERBEROS MSTR   1   14Sep2000 R##SLIN  ADM@SRV.*
__ DFHSM    DFHSM        tDSu SYS1     MSTR   1   14Mar2002 R##SLIN  DFHSM.*
__ DFHSMAUX DFHSM        tDSu SYS1     MSTR   1   12May2000 C##BMR1  DFHSMAUX.*
__ ZFS      DFSUSR        DSu DFSGRP   MSTR   1   18Jul2002 R##SLIN  ZFS.*
__ FWKERN   FWKERN        DSu FWGRP    MSTR   1   20Jul1998 R##SLIN  FWKERN.*
__ ICAPFLOG FWKERN        DSu FWGRP    MSTR   1                      ICAPFLOG.*
__ ICAPPFTP FWKERN        DSu FWGRP    MSTR   1                      ICAPPFTP.*
__ FWKERNP3 FWKERNP3      DSu FWGRP    MSTR   1   31Jul1998 R##SLIN  FWKERNP3.*
__ HODSRV   HOD           DS  SYS1     MSTR   1   13Dec2000 C##BERT  HODSRV.*
__ MVSKERB  MVSKERB       DSu KERBEROS MSTR   1   05Sep2000 R##SLIN  MVSKERB.*
__ RACFOFF  RACFUSR   s   DS  SYS1     MSTR   1   26Jul2002 R##SLIN  RACFOFF.*
```

Figure 241. Started Task protection report - overview panel

The summary line at the top shows the complex name (which database) and system name with time stamp, and the number of started procedures for this complex. When multiple complexes are connected, you first have to select a complex to see this overview.

The display contains the following fields of interest.

Table 184. Started Task Protection report overview panel - field descriptions

Field	Description
Complex	The complex name for the security database.
System	The SMF system ID. Each system can have its own Started Procedure Table ICHRIN03, even while sharing the RACF database.
Timestamp	The time stamp of the database or unload used.
Count	The number of started task entries shown.
Procname	The name of the procedure JCL member in the procedure library. This name is used on the START command to start the task.
Userid	The `userid` assigned by a STARTED profile. This column can contain *, which is the default RACF user ID for a task originating from within the system. Issue the SUPPRESS ID=* to suppress these report lines. For an invalid STARTED profile, this column can contain the JES user ID *undefined*' user, by default ++++++++.

Table 184. Started Task Protection report overview panel - field descriptions (continued)

Flags	Special authorizations or conditions for the started task, coming from the RACF user profile or from the STARTED profile. A character can be displayed at a specific column. Possible characters are: * . An unusual condition exists for this task, a mismatch in a table or database for example. Use the VERIFY STC command to troubleshoot the problem. *r*. The user assigned to the started procedure is revoked. Depending on your RACF and PTF level, the task either cannot be started because it is revoked, or it is running with reduced functionality. *s*. System-wide SPECIAL authority. *o*. System-wide OPERATIONS authority. *a*. System-wide AUDITOR authority. *p* The task is privileged, which means that all RACHECKs are permitted without an audit trail. *t*. The task is trusted, which means that all RACHECKs are permitted but with an audit trail. *D*. The current connect group is the user's default group. *S*. The procedure uses a RACF STARTED profile. *3*. The procedure uses ICHRIN03. *u*. The started task user ID is unprotected, so it can be used to log onto the system.
Group	The current connect group that is used if the task is started.
Subs	The subsystem name the output line applies to. The START command can be issued with this subsystem name in the SUB= parameter. The SUB= parameter is required to direct the START command to a subsystem other than the default (primary) subsystem.
Lib	The sequence number of the procedure library in the concatenation. Each subsystem on each system can have its own concatenation.
h	Indicates that a JCL member is hidden by a member with the same name in a procedure library in front of this library. When the Subs column indicates +, the detail display shows for which subsystem(s) the member is hidden.
Last updt	The last modification date in the ISPF statistics of the JCL member.
By	The user ID present in the ISPF statistics of the JCL member.
STARTED profile	The RACF STARTED profile, if one is found.
UACC	The consolidated universal access of the procedure library. This takes into account the data set profile, the warning mode, the global access table, and the PROTECTALL setting.
Volume	The DASD volume serial where the procedure library resides.

Table 184. Started Task Protection report overview panel - field descriptions (continued)

Dataset	The data set name of the procedure library containing the JCL member for the started task.

If more than one value applies, the **Subs Lib** columns shows + +. The applicable values are listed on the detail display.

Table 185 lists the available action commands.

Table 185. Started Task Protection panel - Available action commands

Command	Description
B - Browse proclib member	Browse the selected procedure using the ISPF BROWSE service.
L - RACF listuser command	Generates a RACF `LISTUSER` command for the STC user ID. Results are presented in a temporary file that you can navigate through using scroll keys or find commands. The default RACF user `*` and the undefined user `++++++++` cannot be listed.
S - Show additional information	Shows additional information for the started procedure. The extra information can include subsystem names, whether the member is hidden by a member with the same name in a procedure library, and the sequence number of the procedure library in the proclib concatenation.
V - View proclib member	View the selected procedure using the ISPF VIEW service.

GLBW - Globally writable data reports

These reports show the z/OS data sets and z/OS UNIX files (zSecure Audit for ACF2 only) that can be updated by almost any user. The GLBWDSN report shows the data sets that are vulnerable to trojan horse and backdoor attacks. The GLBWUNIX report is a UNIX equivalent of the same report.

Background

Hackers often exploit files that can be updated by anybody to increase their authority. For example, they change an executable, source, or parameter file in the hope that it is used by a user with more authority than their current, possibly stolen user ID. This is called a trojan horse attack.

The trojan horse can give the stolen user ID more authority, or change yet another program to install a back door that grants access to the hacker even after the global write condition has been removed.

Globally writable UNIX directories are also a prime way to spread viruses. Countermeasures to protect the UNIX environment are to limit globally writable files so that only well understood applications like `/var` and `/man` are globally writable and to make sure that authorized users for the current directory do not have globally writable files in their search path.

Auditing globally writable data

Figure 242 on page 349 shows a sample GLBWDSN display panel with information about data sets vulnerable to trojan horse and back door attacks.

```
Data sets vulnerable to trojan horse & back door attacks          Line 1 of 14
Command ===> _____________________________________________ Scroll===> CSR
                                                 15 Sep 2000 00:07
   Complex  Timestamp         Profiles HighAcc
   TODAY    15 Sep 2000 00:07       14 ALTER
   Profile key / data set name                  Volume Access  Via      When
s_ CATALOG.UCAT.**                                     UPDATE  - UACC -
__ C##AROB.TESTUACC                                    UPDATE  - UACC -
__ C##BMR1.T.**                                        ALTER   - WARN -
__ C##BWTK.PLANAUTH                            SM3003  UPDATE  - UACC -
__ C##QA.R.READWARN.**                                 ALTER   - WARN -
__ C##QARUN.ACCESS.SYSLOW.**                           ALTER   - WARN -
__ C##QARUN.ACCESS.WARNING.**                          ALTER   - WARN -
__ ONEQUAL.**                                          UPDATE  - UACC -
__ ONEQUAL.SMPMCS                                      UPDATE  - UACC -
__ R##PROB.TEST10                              DISK10  UPDATE  - UACC -
__ R##PROB.TEST10                              JAN     UPDATE  - UACC -
__ R##PROB.TEST10                              PIET    UPDATE  - UACC -
__ SYS1.BRODCAST                                       UPDATE  - UACC -
__ USERCAT.**                                          UPDATE  - UACC -
****************************** BOTTOM OF DATA ********************************
```

Figure 242. Auditing globally writable data - Data set vulnerability report

Table 186 list the fields of interest in for the Data set vulnerability report.

Table 186. Auditing globally writable data - Data set vulnerability report

Field	Description
Complex	The complex name for the security data sources.
Timestamp	The date and time to which the information pertains
Profiles	The number of profiles for which information is available
HighAcc	The highest general access found
Profile key / data set name	The profile reported on
Volume	Volume serial (for a discrete profile)
Access	The access level any user has.
Via	List the reason that access is granted. The value can be any of the following: • Access list entry • *-UACC-* (Universal access level) • *-WARN-* (Profile in warning mode) • *-UNPROT-* (No profile and no protection by default)
When	If the data set has conditional access, the class and resource name are required.

Select any profile to see what resources it protects.

```
Data sets vulnerable to trojan horse & back door attacks          Line 1 of 25
Command ===> _____________________________________________ Scroll===> CSR
                                          15 Sep 2000 00:07
   Profile key / data set name            Volume Access  Via      When
   CATALOG.UCAT.**                               UPDATE  - UACC -
  Type    Profile key / data set name            Volume
  GENERIC CATALOG.UCAT.**
   clustr CATALOG.UCAT.C##CAT                    SYS102
    index CATALOG.UCAT.C##CAT.CATINDEX           SYS102
    data  CATALOG.UCAT.C##CAT                    SYS102
   clustr CATALOG.UCAT.DLIB                      SM3009
    data  CATALOG.UCAT.DLIB                      SM3009
    index CATALOG.UCAT.DLIB.CATINDEX             SM3009
   clustr CATALOG.UCAT.USS                       UNIX01
    index CATALOG.UCAT.USS.CATINDEX              UNIX01
    data  CATALOG.UCAT.USS                       UNIX01
   clustr CATALOG.UCAT.VCNSL01                   CNSL01
    data  CATALOG.UCAT.VCNSL01                   CNSL01
    index CATALOG.UCAT.VCNSL01.CATINDEX          CNSL01
   clustr CATALOG.UCAT.VEPR13H                   EPR13H
    index CATALOG.UCAT.VEPR13H.CATINDEX          EPR13H
    data  CATALOG.UCAT.VEPR13H                   EPR13H
   clustr CATALOG.UCAT.VEPR240                    n/a
    data  CATALOG.UCAT.VEPR240                   EPR240
    index CATALOG.UCAT.VEPR240.CATINDEX          EPR240
   clustr CATALOG.UCAT.VSYSP01                   SYSP01
    data  CATALOG.UCAT.VSYSP01                   SYSP01
    index CATALOG.UCAT.VSYSP01.CATINDEX          SYSP01
   clustr CATALOG.UCAT.VTSTRES                   TSTRES
    index CATALOG.UCAT.VTSTRES.CATINDEX          TSTRES
    data  CATALOG.UCAT.VTSTRES                   TSTRES
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Field	Description
Type	Profile type: • *GENERIC* • *VSAM* • *NONVSAM* • *MODEL* • *TAPE* • *missing* (Indicates that data sets are not protected.)lowercase shows data • *lowercase* (Shows data set resources. For more information, see the table in "SENSPROF - Sensitive Data by Profile report" on page 321).
Profile key / Data set name	Profile key, optionally followed by names of data sets covered by this profile.
Volume	For a discrete profile, the volume serial of the data set.

For UNIX, global write access is of special interest for the following types of files:

- Files with APF, SETUID, or SETGID authorization.
- Files that run program controlled.
- Some special (configuration) files and directories.
- Files that serve a specific function for a user, a profile for example.
- User home directories.

When you configure this option, verify that /tmp variable has the sticky bit on for protection against removal of file and directories owned by other user IDs. For a list of the possible audit concerns, see “UNIX: UNIX System Services File System” on page 1480.

A sample GLBWUNIX display is shown in the following figure.

```
UNIX files vulnerable to trojan horse & back door attacks         Line 1 of 14
Command ===> _____________________________________________ Scroll===> CSR
                                              15 Sep 2000 00:07
   Pri Complex  System      Files
    22 TODAY    DINO         2031
   Pri    Files FS mount point
s_  22        2 /u
__  11       31 /
__  10        3 /etc
__  10        6 /tmp
__  10        1 /u/automount/c##arob
__  10        7 /u/automount/c##asch
__  10       14 /u/automount/c##bert
__  10      234 /u/automount/c##blu1
__  10        3 /u/automount/c##bmr1
__  10        2 /u/automount/c##bmu1
__  10     1722 /u/automount/c##boon
__  10        4 /u/automount/c2eaudit
__  10        1 /u/automount/c2rnew
__  10        1 /u/automount/r##slin
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest.

Field	Description
Pri	The highest audit priority for any audit concern for the system.
Complex	The complex name.
System	The system name.
Files	The number of globally writable UNIX files in the system.
Pri	The highest audit priority for any audit concern for a mount point.
Files	The number of globally writable files in the file system.
FS mount point	The directory at which the file system is mounted.

Select any mount point to see the world writable files in it.

```
UNIX files vulnerable to trojan horse & back door attacks          Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
                                              15 Sep 2000 00:07
   Pri Complex  System      Files
    22 TODAY    DINO         2031
   Pri    Files FS mount point
    22        2 /u
   Pri T FileMode  + apsl AuF Owner    Group    Relative pathname (within FS)
__  22 - -w--w--w-   --s  fff C##QA100 Zsecur   c##qa100/.profile
__  10 d rwxrwxrwx        fff C##QA079 C##QA    sub1/sub2/sub3/sub4/sub5/sub6/sub
****************************** BOTTOM OF DATA ********************************
```

The layout of this report is identical to that of the UNIX reports for authorized files, see “APFPROT - Authorized Programs reports” on page 328.

UIDNOUSR - UNIX ids used in the file system, but not defined to RACF

This report, and the related GIDNOGRP for groups, report on the usage of UIDs and GIDs that are owners of data in the file system, but are not defined in the RACF database. This could result in extra, unintended access being granted when the UID or GID in question is assigned to a user or group.

Auditing undefined UIDs

A sample display is shown in the following figure.

```
UIDs not defined in the complex                                  Line 1 of 3
Command ===> _____________________________________________ Scroll===> CSR
                                              8 Mar 2001 00:07
   Files Complex  System
       3 DINO     DINO
   Files User id
__     1        123
s_     1       1112
__     1      65535
****************************** BOTTOM OF DATA ********************************
```

This display contains the following fields of interest:

Field	Description
Files	The number of undefined UIDs found.
Complex	The complex name.
System	The system name.
Files	The number of occurrences of this UID in the file system.
User id	The user ID found.

Select any UID to see the files it owns, summarized per mount point:

```
UIDs not defined in the complex                                  Line 1 of 3
Command ===> _____________________________________________ Scroll===> CSR
                                              8 Mar 2001 00:07
   Files Complex  System
       3 DINO     DINO
   Files User id
       1       1112
   Files FS mount point
       1 /
   T FileMode  apsl AuF Group    Relative pathname (within FS)
__ - rw-rw-rw- --s  fff OMVSGRP  var/man/C/ls.1.bpxa5mst
****************************** BOTTOM OF DATA ********************************
```

The display contains the following fields of interest:

Field	Description
Files	The number of occurrences of this UID in this file system
FS mount point	The mount point.
T	The file type.
FileMode	The effective file mode
apsl	The effective extended attributes.

Field	Description
AuF	The combined audit files.
Group	The group that is associated with this file.
Relative pathname (within FS)	The relative path name for this file from the mount point of the file system.

The layout of the detail report is identical to that of the UNIX reports for authorized files. See "APFPROT - Authorized Programs reports" on page 328.

Auditing undefined GIDs

The GIDNOGRP report is virtually identical to the UIDNOUSR report described in "UIDNOUSR - UNIX ids used in the file system, but not defined to RACF" on page 352. Only UID and GID, and owner and group are exchanged for each other.

AU.V VERIFY - Verify Selection List

The `VERIFY` command is described in "VERIFY" on page 942. It combines profile data with resource descriptions, and reports on inconsistencies. `VERIFY` also generates commands to fix some inconsistencies. If a `CKFREEZE` is present, `VERIFY PERMIT` supports resource deletion, which means that the data sets covered by a profile that is removed are themselves removed as well.

You can use any number of `VERIFY` selections in one run, or select just one, by selecting the fields as shown in Figure 243. All but the first few selections require a `CKFREEZE` file.

```
  Menu  Options  Info  Commands  Setup          StartPanel
------------------------------------------------------------------------------
                        zSecure Suite - Audit - Verify
Command ===> ____________________________________________________________

Enter "/" to select one or more options
_  Permit            Find undefined users and groups and their profiles

_  User permit       Find and remove redundant permits to userids
_  Connect           Compare USER, GROUP and CONNECT profiles
_  PADS              Programs on conditional access list have PROGRAM profile
_  Group tree        Loops in grouptree
_  Password          Userids with trivial passwords (not from an unloaded db)
_  Protect all       All datasets are protected by a (discr or gen) profile
_  On volume         Datasets defined by discrete profiles actually exist
_  Not empty         Generic profile has matching disk or tape datasets
_  All not empty     As above, even 'outer' generic profiles
_  Indicated         Discrete profile exists for RACF-indicated datasets
_  Program           Datasets as members in PROGRAM profile exist on disk
_  Pgm exists        PROGRAM profiles cover actual load modules
_  Started task      Check that procedures can indeed be started, etc.
_  TSO all RACF      All TSO users should have RACF password and TSO segment
_  Sensitive         Sensitive datasets not protected properly
_
```

Figure 243. Audit Verify Command

The verify option selection panel is followed by customization panels. You can use the first panel shown in Figure 244 on page 354 to change the output sort order and to suppress output that you do not want to include in the report.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite Verify
Option  ===> ____________________________________________________________

Complete any of the selection criteria below and press ENTER
Enter "/" to select sort option
  _  Message        - Sort output lines by message type (default)
  _  Volume         - Sort output lines by volume serial and dataset name
  _  Dsname         - Sort output lines by dataset name
  _  Program        - Sort output lines by program name (AC1, PADS and STC

  _  Suppress FALLBACK (do not flag unused ICHRIN03 entries)
  _  Simulate program control mode . . ENHWARN     (BASIC,ENHANCED or ENHWARN)

Limit amount of output
 Message limit  . . 50______     Message limit per volume
 Suppress msg (4 digit message numbers to ignore, separated by commas)
                    ____________________________________________________
 Suppress vol (messages for these disk volumes can be ignored)
                    ______ ______ ______ ______ ______ ______ ______ ______
 Suppress id (userids to be suppressed (e.g. * and ++++++++))
                    ________ ________ ________ ________ ________ ________
```

Figure 244. Verify - customize sort order and suppress output

The sort options are mutually exclusive. The SUPPRESS FALLBACK option applies only to VERIFY STARTED TASK; it means that entries in Started Procedure Table ICHRIN03 are only taken into consideration if there is no overriding profile in the STARTED class for a started task.

The other suppress options should be self-explanatory.

You can use the **Simulate program control mode** to simulate the mode in which RACF program control runs (z/OS 1.4 and up). This option applies only to VERIFY PADS. Note that * and +++++++ are the default user IDs under which a started task can be run when there is no ICHRIN03 or STARTED match, respectively.

A subsequent panel might open asking you whether data sets and ID-specific general resource profiles are to be removed if the ID does not exist anymore. You can also specify up to 8 classes to be excluded from processing.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite Verify
Option  ===> ____________________________________________________________


Delete profiles as well as datasets when removing undefined ids?

Enter "/" to generate delete command for:

  /  Dataset and id-specific profiles   (enables next 3 options)
  /  Datasets and their catalog entries (enables next 2 options)
  /  Catalog entries without datasets
  /  Uncataloged datasets

Suppress class(es) . . ________ . . ________ . . ________ . . ________
                       . . ________ . . ________ . . ________ . . ________

                       Press ENTER to start the VERIFY commands
```

Figure 245. Verify - remove obsolete profiles

After the VERIFY has completed, the results are shown. If commands were generated, the CKRCMD file is shown first. Otherwise, the SYSPRINT file is displayed.

If more than one complex exists in the currently selected input file sets and commands are generated, the CKRCMD selection panel shown in Figure 246 opens:

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                       zSecure Suite - Result  Use END for other files
COMMAND ===> _____________________________________________ Scroll ===> CSR_

The following selections are supported:
 B Browse file               S Default action (for each file)
 E Edit file                 R Run commands
 P Print file                J Submit Job to execute commands
 V View file                 W Write file into seq. or partitioned data set
 M Mail file

CKRCMD for the specified environments:

   Complex   Njenode   Rrsfnode   System              #Lines
 _ DINO      <LOCAL>   THESRRSF   DINO                29
 s DD971028  CRM4      C##4       C##4                14
****************************** Bottom of data ********************************
```

Figure 246. CKRCMD selection panel

Figure 247 shows commands were generated by specifying VERIFY PADS PERMIT CONNECT. See "VERIFY" on page 942 for more information.

```
 File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       C##BDV1.C2R2EF2A.CKRCMD                    Columns 00001 00072
Command ===> _____________________________ Scroll ===> CSR_
****** ***************************** Top of Data ******************************
000001         /* CKRCMD file CKR5CM2 complex C##4 NJE C##4 generated 15 Oct 20
000002          /* Commands generated by VERIFY PERMIT     */
000003         rdelete SURROGAT NOTEXIST.DFHINSTL
000004         rdelete SURROGAT NOTEXIST.DFHSTART
000005         rdelete JESSPOOL &RACLNDE.C##QAC4.**
000006         altdsd 'C##BERT.OWNER#IS.MAGWEG' generic nonotify
000007         altdsd 'C##BERT.OWNER#IS.MAGWEG' generic owner(C##BERT )
000008         altdsd 'C##QARUN.NOOWNER.**' generic owner(C##QARUN)
000009         connect NVUSR10  group(SYS1    ) owner(SYS1    )
000010         permit 'C##AROB.**' generic delete id(CRUNDEF )
000011         permit 'C##AROB.TEST' generic delete id(CRUNDEF )
000012         SETROPTS REFRESH RACLIST(SURROGAT) /* POSIT 104 */
000013         SETROPTS REFRESH GENERIC(JESSPOOL) /* POSIT 110 */
000014         SETROPTS REFRESH GENERIC(DATASET)
****** **************************** Bottom of Data ****************************
```

Figure 247. Generated commands for VERIFY PADS PERMIT CONNECT operation

After you leave the SYSPRINT or CKRCMD file, the standard Results panel is shown, see "RESULTS - View output and results" on page 24. You can use this panel to view the other output generated by Security zSecure. For instance, selecting SYSPRINT results in a display of the messages. Figure 248 on page 356 shows a sample of the SYSPRINT output for a VERIFY PADS PERMIT CONNECT operation.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY PADS PERMIT CONNECT
End of  CKRCMDV  (include level 1)

-------------------------------------------------------------------------------------------------------------------------------
V S A M   O R   V V D S   I N C O N S I S T E N C I E S  25 Mar 2007 00:05                                          page 5

CKR0292 08 Connected catalog not found on any volume                  USERCAT.MVSV5D
CKR0073 08 Catalog not found on any volume on any system              CAT1.M9106.UITWIJK.#01
-------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   C O N N E C T          25 Mar 2007 00:05                                          page 6

CKR0067 08 Missing connect  NONEXI2U to group CRMCXDEL
CKR0067 08 Missing connect  NONEXI2U to group NONEXI2
-------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   P A D S                25 Mar 2007 00:05                                          page
7
CKR1203 04 BASIC or MAIN not specified on program profile CAT      used in dataset profile C##BERT.PADS.**
CKR1204 04 No specific program profile found for program PROGRAM1 used in dataset profile C##BSG1.E307011.TEST
-------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   P E R M I T            25 Mar 2007 00:05                                          page 8

CKR0068 00 Undefined id -   C##QAWAY referenced       1 times
CKR0261 04 Key with unknown C##QAWAY general resource profile SURROGAT NOTEXIST.DFHINSTL
CKR0057 04 Undefined owner  C##QAWAY of generic dataset profile       C##QARUN.NOOWNER.**                          - make C##QARUN
CKR0062 04 Undefined owner  C##QAWAY  connect  NVUSR10  to group SYS1
CKR0050 04 Undefined permit C##QAWAY  in access list generic dataset    C##AROB.**
```

Figure 248. Sample SYSPRINT for VERIFY PADS PERMIT CONNECT

Common RACF problems

The standard RACF product includes utilities and commands to handle most of the situations which security administrators, auditors, and technical staff are likely to encounter. However, some of these facilities are difficult to use or take too long to consider using them on a daily basis. As a result of this, some installations have been forced to develop their own procedures for dealing with these situations and others have been unable to afford the resources to deal with them on a regular basis.

This section of the manual shows how Security zSecure can be used to provide fast solutions to some of the most common problems facing RACF users today in four major areas:

USER/GROUP Maintenance

- Finding user/group/connect inconsistencies (ensures USER, GROUP, and CONNECT profiles in synchronization)

PROGRAM Class Maintenance

- Checking for obsolete conditional access lists (when PROGRAM profiles have been removed)
- Checking for program/data set referential integrity (finds non-existent data set/volume PROGRAM combinations)
- Checking for program/load module referential integrity (finds PROGRAM profiles not describing any physical module)

DATASET Maintenance

- Finding and protecting unprotected data sets (checks for possible unrecorded access depending on the current PROTECTALL setting)
- Removing unused discrete profiles (resulting from volume-level operations)
- Finding and removing redundant discrete profiles (after conversion from ADSP to generic environment)

- Removing unused generic profiles (after deletion of 'subject' data sets)
- Converting to generic profiles (Security zSecure commands to assist in conversion to generics)
- Finding and resetting unnecessary RACF-indicated bits (where no discrete profile exists)

STARTED Class Maintenance

- Finding inconsistencies in started task definitions.

Checking for obsolete conditional access lists

RACF offers the possibility to grant access to data sets only through specific programs. This facility is called Program Access to Data Sets (PADS). This is done by having an extra access list on the data set profile called the *conditional access list*. The conditional access list consists of entries containing an *id*, an *access level*, and a *program name*. For the entry to be effective, the program name must be defined as a profile in the class PROGRAM, and the user must call the program from a 'clean' environment.

The problem is that no check is made by RACF on the existence of the PROGRAM profile, neither when setting the conditional permit, nor when deleting a PROGRAM profile. Most users have discovered this by trying to debug 913 abends for PADS data sets, e.g. due to a typing error in the program name on the conditional access list. A more serious problem is introduced if the PROGRAM profiles (and presumably the programs, too) are removed from the system. A conditional access list entry then exists that serves no function anymore, a so-called *obsolete conditional access list entry*.

Depending on the procedures around the use of the PROGRAM class, this can result in a *security exposure*. The exposure exists because a data set profile gives access based on a program name that is undefined. Anybody with class authorization for PROGRAM can define the program profile, indicating a program in his own load library. He then has access to somebody else's data set.

Security zSecure provides a function specifically designed to report and remove obsolete conditional access list entries. The report is created by means of the following command (option **AU.V**):

```
VERIFY PADS
```

Figure 249 gives an example of the relevant parts of the output. Note that the query also specifies a global exclude of the catch all profiles * and ** (via SETUP PREAMBLE), because in a database with such catchalls no output would otherwise have been generated! Messages displayed depend on the program security mode.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    5 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY PADS
End of  CKRCMDV  (include level 1)

------------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   P A D S                25 Mar 2007 00:05                                                  page 5

CKR1203 04 BASIC or MAIN not specified on program profile CAT      used in dataset profile C##BERT.PADS.**
CKR1204 04 No specific program profile found for program PROGRAM1 used in dataset profile C##BSG1.E307011.TEST
```

Figure 249. Sample VERIFY PADS output

To generate commands to remove the obsolete entries, the CKRCMD file must be allocated.

The commands generated can be longer than 72 characters. You can use the default CLIST format (VB 255).

Checking for program existence

Profiles in the class PROGRAM can contain data set name/volume combinations as members. RACF does not check on the existence of these data sets, either during profile creation, or during data set deletion. This can easily lead to superfluous and inconsistent database entries.

One type of inconsistency can occur if a load library is moved to another volume, by SMS for example. If the library is no longer listed in a `PROGRAM` profile because of its new volume, 913 abends occur when using Program Access to Data Sets (PADS) with this program from this library.

In addition, a *security exposure* results if the program-protected library is part of the Authorized Program Facility (APF). It is common procedure to protect sensitive utilities in the MVS LNKLST concatenation with PROGRAM profiles. Utilities can be considered *sensitive* if they have the ability to circumvent RACF. To have this potential, utilities must be part of an APF library and linked with AC=1. Now if the APF library containing the sensitive utility is moved to another volume, then access to its function is not restricted anymore based on the access list of a PROGRAM profile, unless the PROGRAM profile is updated to contain the new volume.

Security zSecure provides a function designed to report and remove data set/volume combinations that do not exist or are otherwise invalid (data set is not partitioned, volume is not mounted or is not a z/OS readable disk). It also provides a function designed to report and remove PROGRAM profiles that are not actually protecting any program in any data set. Note that for the APF problem described above, removal of the old combination is not enough - the new combination should be added as well.

If you have allocated a CKRCMD file, RACF commands to remove the invalid PROGRAM profiles and members are generated. Because commands can be longer than 72 characters, use the default CLIST format (VB 255).

Before running the generated commands, review them to make sure that the results are what you intended. The analysis that leads to the generation of REMOVE or DELMEM commands is primarily focused on security. Executing the commands blindly can lead to availability problems. The correct remedy might be restoring datasets instead of removing the profiles or members. When in doubt, consult your systems programmer.

The following CARLa command (found in the interactive interface as AU.V - Program) checks the validity of the specified PROGRAM profile members:

```
VERIFY PROGRAM
```

This function requires a CKFREEZE file.

Figure 250 on page 359 gives an example of the relevant parts of the SYSPRINT from running this command:

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY PROGRAM
End of  CKRCMDV  (include level 1)

-------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   P R O G R A M           25 Mar 2007 00:05                                                page 5

CKR1250 04 PROGRAM data set name is obsolete                C##4     POSTNEW1 -        SYS1.NO.DATASET
           Partitioned data set does not exist on any volume and system               SYS1.NO.DATASET
CKR0044 04 PROGRAM dsn/vol obsolete                         C##4     CNA*     - C##001 C##A.D.CNRNEW.CNRLOAD
           Volume is not mounted on system             C##4                    C##001
CKR1252 04 PROGRAM IPL volume entry dsn/****** obsolete     C##4     CNRACF   - ****** C##A.C##PROD.LOAD
           Data set not on IPL volume of system        C##4                    OS39R1 C##A.C##PROD.LOAD
```

Figure 250. Sample VERIFY PROGRAM output

VERIFY PROGRAM can issue messages indicating why a member could be removed from a PROGRAM profile, or that information is missing to decide on that. There are several messages for indicating the various conditions. VERIFY PROGRAM also flags volume-specific members that are made redundant by a member without a volume specification. If the messages indicate that information is missing, you should investigate why, solve the problem(s) and rerun VERIFY PROGRAM. See also “VERIFY PROGRAM, PGM” on page 950.

The following CARLa command (found in the interactive interface as AU.V - Pgm exists) checks the existence of load modules in the libraries indicated by the PROGRAMprofile members:

```
VERIFY PGMEXIST
```

This function requires a CKFREEZE file.

Figure 251 gives an example of the relevant parts of the SYSPRINT from running this command:

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY PGMEXIST
End of  CKRCMDV  (include level 1)

-------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   P G M E X I S T         25 Mar 2007 00:05                                                page 5

CKR0296 04 PROGRAM profile w/o load module but info missing  C##4     RACTRACE
           PDS directory not in CKFREEZE for data set   C##4                    M95DR2 SYS1.C##.LINKLIB
CKR0297 04 Obsolete PROGRAM, load module not in libraries    TEST     ABEND806
```

Figure 251. Sample VERIFY PGMEXIST output

VERIFY PGMEXIST can issue messages CKR0296 and CKR0297. The former indicates that the PROGRAM profile does not protect any load module (and generates a command to remove the profile). The latter indicates that the PROGRAM profile does not seem to protect any load module, but some information necessary to conclude that is missing. In this case, a command to remove the PROGRAM profile is generated, but it is commented out. You should investigate why the indicated information is missing, solve the problem(s) and rerun VERIFY PGMEXIST. See also “VERIFY PGMEXIST, PROGRAMNONEMPTY, PROGRAMNOTEMPTY, PGMNONEMPTY, PGMNOTEMPTY” on page 949.

Finding and protecting unprotected data sets

It is possible that data sets exist in the system that are not matched by any profile in RACF. If the RACF indicated bit of these data sets is off, access to the data sets is governed by the setting of the system-wide RACF option PROTECTALL. (Data sets with their RACF indicated bit on are discussed in Finding and resetting unnecessary RACF indicated bits).

If PROTECTALL(FAIL) is active, access is only granted to user IDs with SPECIAL authority and for user IDs equal to the first qualifier of the data set name. We call these data sets *inaccessible* data sets. If PROTECTALL(FAIL) is not active, access is granted to any user ID, even for user IDs not defined to RACF. We call these data sets *unprotected*. If the RACF indicated bit is on and no generic or discrete profile is found matching the data set, RACF denies all access which makes these data sets inaccessible.

In all cases, it is useful to identify the data sets not protected by any profile. In a PROTECTALL environment, a data set might be unprotected because a generic profile was removed prematurely without first deleting or renaming the data sets. In a non-PROTECTALL environment, data sets might be unprotected even though your standards dictate protection.

Security zSecure provides a function to identify all data sets without generic or discrete profiles. This function is requested by selecting option **AU.V**, Protect all, or by issuing the following command.

```
VERIFY PROTECTALL
```

If a RACF indicated data set has no discrete or matching generic profile, Security zSecure generate commands to create discrete profiles for these data sets. However, most of the time you might not want to create discrete profiles. It is better to define a generic profile and configure PERMITs for the groups requiring access. Generated commands are written to the `CKRCMD` file.

A `CKFREEZE` file is required for this function.

Figure 252 gives an example of the relevant parts of the SYSPRINT from running this command:

```
Include CKRALLOC (ISPF variable)
     2 |/* Data from DD070525 */
     3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
     4 |
     6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
     7 |
     9 |alloc type=CKRCMD DD=CKR02CMD
 End of  CKRALLOC (include level 1)

 Include CKRCMDV  (ISPF variable)
     1 |VERIFY PROTECTALL
 End of  CKRCMDV  (include level 1)

------------------------------------------------------------------------------------------------------------------------------------------------------
                                                                                                                                          page 4

 CKR0097 00 Z5DB22 has 51 inaccessible dataset(s) (not indicated, no profile)
 CKR0091 08 Z7DB81 message limit exceeded - 572 detail message(s) suppressed
------------------------------------------------------------------------------------------------------------------------------------------------------
 M E S S A G E S   V E R I F Y   P R O T E C T A L L      25 Mar 2007 00:05                                                                   page 5

 CKR0082 04 Inaccessible dataset (not indicated and no generic)  SME004 C##QARUN.RRSFLIST
 CKR0082 04 Inaccessible dataset (not indicated and no generic)  WORKPK @@.TEST.DIT.MET.REP.SENS
```

Figure 252. Sample VERIFY PROTECTALL output

Note that the error messages on data set level are preceded by summary messages per volume. You can modify the order of the messages by means of the BY parameter of VERIFY. See “VERIFY” on page 942.

The present version of the product does not support this verification for data sets that are only known to CA1, RMM, and TLMS.

If Automatic Backup and Recovery (ABR) is used with the PROFKEEP option, a discrete profile for a migrated non-VSAM data set is assumed to protect it. This assumption is incorrect if the data set does not have the RACF indicated bit on; to verify whether this is the case, however, would necessitate investigating the migration copy, to which end all the migration (DASD and) tapes would have to be investigated. This might be a very time consuming process and is not supported in the present version of the product. Note that most installations with ABR do not use this option.

Removing unused discrete profiles

When operating an Automatic Data Set Protection (ADSP) environment, sooner or later a number of discrete profiles exist for which no corresponding data set is available. This happens mostly through volume-level operations for which authorization is granted by APF and often in addition by checks in the DASDVOL class. These volume-level operations often do not support discrete profiles. The problem is not necessarily limited to ADSP environment. For example, by default without special RACF exit processing), any user can specify PROTECT=YES in his JCL and/or issue the ADDSD command, at least for data sets starting with his `userid`, and for group data sets if he is connected with CREATE authority.

The unused profiles exist mostly unnoticed in the RACF database. If the volume name is reused and a user tries to allocate a data set for which a profile was left over, the following error message is generated: `RESOURCE ALREADY DEFINED`.

The situation can be highly misleading if a data set exists on the volume with the RACF indicated bit off, which means that DFP does *not* request a search for a discrete profile while at the same time a discrete profile does exist. The RACF LISTDSD command lists the discrete profile for the data set even though the profile is not used for access decision with regard to the data set.

Some security specialists call this a *security exposure*, because users might try to restrict access to the data set by modifying the access list of the discrete profile, while in reality access is *not* restricted due to the fact that DFP only checks the generic profile.

Security zSecure provides a function for reporting and removing the unused discrete profiles. The command to accomplish this is (option **AU.V**):

```
VERIFY DATASET
```

The function is called like this because it verifies that a data set is present for each discrete profile. An equivalent (alias) command, which is easier to remember, is:

```
VERIFY ONVOLUME
```

A CKFREEZE file is required for this function.

If Automatic Backup and Recovery (ABR) is used with the PROFKEEP option, a discrete profile for a migrated non-VSAM data set is assumed to protect it. This assumption is incorrect if the data set does not have the RACF indicated bit on; to verify whether this is the case, however, would necessitate investigating the migration copy, to which end all the migration (DASD and) tapes would have to

be investigated. This might be a very time consuming process and is not supported in the present version of the product. Note that most installations with ABR do not use this option.

Relevant parts of the output from this command are shown in Figure 253. The error messages distinguish three cases: no data set present on volume, volume not mounted, and data set present but not RACF-indicated. In addition, summary messages per volume are printed.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY ONVOL
End of  CKRCMDV  (include level 1)
------------------------------------------------------------------------------------------------------------------------------------------
CKR0095 00 DISK10 has 1 discrete profile(s) but volume not mounted
CKR0095 00 MIGRAT has 3 discrete profile(s) but volume not mounted
CKR0094 00 WORKPK has 1 discrete profile(s) without dataset on the volume
------------------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   O N V O L U M E         25 Mar 2007 00:05                                                    page 5

CKR0042 04 Discrete profile present but no dataset on volume    WORKPK R##SLIN.GEHEIM
CKR0252 04 Multivolume discrete profile but volume not mounted  DISK10 R##PROB.TEST10
CKR0043 04 Discrete profile present but volume not mounted      MIGRAT DFHSM.BACK.T465001.C##BGUS.RACFUD.I7034
CKR0043 04 Discrete profile present but volume not mounted      MIGRAT DFHSM.BACK.T555803.C##ASCH.GDG.I7107
```

Figure 253. Sample VERIFY ONVOLUME output

Commands can be generated to remove the unused discrete data set profiles by allocating the CKRCMD file.

For unused single volume discrete profiles, commands are generated to remove the profile.

For *multivolume* discrete profiles, commands are generated to remove the volumes from the profile that did not contain the data set. If the data set is not present on *any* of the volumes in the profile, the last command generated is refused by RACF, since the profile is not multivolume anymore. A second VERIFY run generates the command to remove this profile.

Removing unused generic profiles

While an environment with generic profiles contains considerably fewer profiles than an all-discrete environment, discrete profiles do have one big advantage over generics: they are deleted when the data set is deleted. The complete ban on discrete profiles (as some sites have done) can lead to a proliferation of generic profiles that have been created for the purpose of setting a permit on one data set, but that have not been deleted when the data set was deleted.

Security zSecure assists in this problem by providing a function that can automatically generate commands to remove *empty* generic data set profiles, for example, data set profiles that are not used for the protection of any currently existing data set. Two options exist for this function: removing *all* empty generic profiles, or only generic profiles also covered by a less specific profile. The last option is generally preferable in a PROTECTALL environment, since removal of the last generic profile potentially covering a new data set will prevent allocation of that new data set.

For the function to perform properly, a CKFREEZE file is required containing VTOC, VVDS, BCS (catalog), HSM MCDS, DMSFILES, ABR, RMM, TLMS VMF,

and CA1 TMC information. *If the catalog information is not present, VSAM data sets are left out, which can increase the number of profiles found to be empty.*

Do not use this function in an ADSP environment with PROTECTALL active because in that case all data sets are covered by discrete profiles, resulting in all generics being considered empty. However, the generics are required in practice to create new data sets with discrete profiles and have them restored from backups.

Likewise, you should be careful in using the ALLNOTEMPTY variant of this function if you use Automatic Backup and Recovery (ABR) with the PROFKEEP option, since the product does not investigate the migration tapes, and hence *assumes* the RACF indicated bit to be set if a discrete profile exists for the data set. If this turns out to be false, the data set might actually be covered by a generic profile that is considered empty.

If you currently do not have the SETROPTS TAPEDSN option active, the existence of tape data sets does not cause the profiles to be considered non-empty. If this is the case, the program prepares for future activation of the TAPEDSN option by including the following command:

```
SIMULATE SETROPTS TAPEDSN
```

This assures that generic profiles that cover only data sets on tape are not deleted.

The function is called by the following command (option **AU.V**):

```
VERIFY NOTEMPTY
```

or, if you are sure that you want to have the *last* generic profile removed:

```
VERIFY ALLNOTEMPTY
```

To generate commands, allocate the CKRCMD file.

Relevant parts of the output from this command are shown in Figure 254.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |SIM SETR TAPEDSN
    2 |VERIFY NOTEMPTY
End of  CKRCMDV  (include level 1)

------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   N O T E M P T Y         25 Mar 2007 00:05                                          page 5

CKR0077 04 Generic profile without matching datasets                  ADM1.SPECIAL.*
CKR0077 04 Generic profile without matching datasets                  ADM1.SPECIAL.*.**
CKR0077 04 Generic profile without matching datasets                  ADM1.SPECIAL.**
```

Figure 254. Sample VERIFY NOTEMPTY output

Finding and resetting unnecessary RACF indicated bits

If a data set is RACF indicated, DFP requests a search for a discrete profile. If the profile is not present, then generic processing is started. The latter process is known as *always-call*: RACF is always called to to search for a generic profile even if the data set is not RACF indicated or if the data set is indicated but no discrete profile was found. [4] . This processing behavior can create unnecessary I/O overhead for data sets that are RACF indicated but do not have a discrete profile.

4. Security zSecure operations presuppose an *always-call* environment. All systems with DFP or DFSMS have always-call.

The normal situation is that the data set is *not* RACF indicated, avoiding the overhead of trying to find a discrete profile in the database before using a generic profile (generics are retained in-storage once referenced).

The situation is typically created by backup/restore operations without a proper RACF interface for discrete profiles, or by conversions to generic profiles that used DELDSD NOSET to remove the discrete profiles. In addition, a number of 'hard cases' can exist that can only be removed by using alternate IPL parameters, like page data sets, and SMF data sets.

Security zSecure provides a function to report on RACF indicated data sets without discrete profiles. This function generates commands to add discrete profiles for these data sets. To properly reset the indicators, these discrete profiles can be removed later on with the REMOVE REDUNDANT command discussed in "Finding and removing redundant profiles" on page 366.

The function to generate the discrete profiles is available from the Audit Verify option (**AU.V**) on the main menu. You can also access the function by issuing the following command:

```
VERIFY INDICATED
```

A CKFREEZE file is required for this function.

If Automatic Backup and Recovery (ABR) is used with the PROFKEEP option, discrete profiles for migrated non-VSAM data sets might or might not be redundant, depending on the RACF indicated bit which cannot be determined without investigating the migration tapes. These profiles are not included in the report.

Relevant parts of the output from this command are shown in Figure 255:

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY IND
End of  CKRCMDV  (include level 1)

------------------------------------------------------------------------------------------------------------------------------------------------------
CKR0092 00 SME003 has 1 RACF indicated dataset(s) without profile
CKR0092 00 WORKPK has 2 RACF indicated dataset(s) without profile
------------------------------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   I N D I C A T E D       25 Mar 2007 00:05                                                                    page 5

CKR0040 04 RACF indicator set but no discrete profile found for SME003 C##BERT.SYS1.CAUNVSAM
CKR0040 04 RACF indicator set but no discrete profile found for WORKPK C##ASCH.TESTGDG.G0002V00
```

Figure 255. Sample VERIFY INDICATED output

The messages in the example are generated in their default order (by message type). You can use the BY parameter of VERIFY to change the order.

Commands can be generated to add discrete data set profiles by allocating the CKRCMD file.

Finding user/group/connect inconsistencies

Information about the user/group structure is stored in the RACF database in a redundant way. To be precise, the RACF database stores the information 3 times:

on the USER profile, on the GROUP profile, and on the CONNECT profile (for non-restructured databases) or in a repeat group in the USER profile (for restructured databases).

Some events can destroy the consistency of these 3 information sources on connects. E.g. the system can go down during a RACF command, or the system can be operating with inconsistent *database range tables* across shared systems.

Security zSecure provides a function to verify the consistency of these 3 information sources. This is done by the following command (option **AU.V**):

```
VERIFY CONNECT
```

The following example examines in a healthy database what problems would be recognized if the base segment of user C##BJTI would somehow become unrecognizable (by instructing the program to pretend it is not there with a global EXCLUDE statement in SETUP PREAMBLE).

Relevant parts of the output from this command are shown in Figure 256.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CNRPRE   (ISPF variable)
    1 |exclude class=user key=c##bjti segment=base
End of  CNRPRE   (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY CONNECT
End of  CKRCMDV  (include level 1)
------------------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   C O N N E C T           25 Mar 2007 00:05                                                    page 5

CKR0067 08 Missing connect  C##BJTI  to group C##B
CKR0066 08 Missing group    C##B     on user C##BJTI
```

Figure 256. Sample VERIFY CONNECT output

No commands are generated by Security zSecure to remedy the situation, since the best course of action depends on a number of factors. For instance, it is undesirable to delete a user profile and add it again if many data set profiles have to be preserved. Sometimes, a sequence of REMOVE and CONNECT commands does the job. Sometimes, however, the BLKUPD utility is needed. If IBMUSER is one of the user IDs involved, carefully study the RACF documentation. Each IPL, the IBMUSER user ID is recreated if it is missing, but this does not necessarily apply to its connects.

Converting to generic profiles

Conversion from an Automatic Data Set Protection (ADSP) environment to a PROTECTALL environment with mainly generic profiles generally includes the following sequence of steps:

1. Decide on access requirements. For instance, batch jobs that use unprotected data sets must be identified, as well as the batch `userid`s used.
2. Make a list of all groups that have ALTER access on a generic DATASET profile that has this same group as the High-level qualifier. Example: SYS1.APF.** might have group SYS1 with ALTER access. This is needed to assure that users that had a connect with CREATE authority do not lose the authority to create new group data sets after PROTECTALL has been activated and their ADSP attribute has been reset. To continue the preceding example, make sure that SYS1.** has SYS1 in the access list with ALTER access.

3. Activate PROTECTALL(FAIL).
4. Remove user or connect ADSP attributes synchronously with removing production JCL steps containing explicit PERMIT commands. This synchronization might be necessary if production JCL uses explicit PERMIT commands to tailor the access list of data sets (and hence, profiles) newly made in previous steps (poor man's profile modelling), and in addition aborts the production job sequence if a nonzero return code is issued (which would be the case if ADSP were turned off globally - the PERMIT command would issue return code 12 because no profile would exist). Using just the system-wide SETROPTS NOADSP instead is possible if all these conversions can be scheduled at the same time or if your production JCL does not contain dependencies on correct execution of RACF commands on discrete profiles - see also the background item below.
5. Remove PROTECT=YES statements in JCL, as well as PROTECT keywords on ALLOCATE commands.
6. Remove discrete profiles with the same properties as the generic profile. These profiles are *redundant*.
7. Define generic profiles for groups of similar profiles not covered by the standard generic profile, and remove the discrete profiles that have become redundant by the addition of the generic profile.

zSecure provides assistance in this process by means of the SELECT ADSP (step 4), REMOVE REDUNDANT (step 5), and REPORT NONREDUNDANT (step 6) commands. These are discussed in “Finding profiles with specific attributes” on page 1684,“RA.3.2 Non redundant - Data set profiles different from less specific profiles” on page 201, and “Finding and removing redundant profiles,” respectively.

zSecure Audit for ACF2 provides assistance in this process by means of the NEWLIST TYPE=SMF. This can be used to trace access to unprotected data sets, including the access level used. See the zSecure Audit for ACF2 CARLa script CKALFNPR.

Background - removing ADSP

With respect to step 4, removing ADSP, you must be aware that this is difficult to perform on a group-by-group basis if you have activated list-of-group processing. The ADSP attribute used by RACF is *not* the ADSP attribute on the CONNECT for which a data set profile is being CREATEd, but instead the ADSP attribute of the *current connect group*.

Finding and removing redundant profiles

Security zSecure provides a function specifically designed to aid in the conversion from ADSP to generic profiles. This is done by automatically generating commands to delete discrete profiles that give *similar* ("equivalent") access to that resulting from the combination of the most specific matching generic data set profile and the most specific matching global table entry (if present).

If you use Automatic Backup and Recovery (ABR) with the PROFKEEP option, you should be aware that on restore of a non-VSAM data set that must be recreated, ABR will request a default discrete profile to be created via ADSP if its RACF indicated bit was set on migration. In addition, this RACF indicated bit is only available on the migration tapes, which currently are not checked; instead it is assumed that an existing discrete will apply. If a data set is already allocated, ABR will fail the restore unless the RACF indicated bits match. Therefore, if you are converting from ADSP to generic profiles, we recommend that you consider the implications regarding ABR *first*, and review the commands generated to remove profiles bearing this in mind.

For a profile to be considered *redundant*, three profile properties are checked:

1. Access requirements (access list, conditional access list, and universal access).
2. Audit requirements (failure audit level, success audit level).
3. Erase-on-scratch requirement.

The last two items are simply compared to those of the most specific matching generic profile, called the *candidate* profile. They must be equal before the profile is considered redundant. However, the *erase-on-scratch* requirement is not checked if the system wide option ERASE(ALL) or NOERASE is active.

The access requirement comparison is more complicated. Simplest is the *universal access* (UACC) comparison. For a profile to be considered redundant, its UACC must either be equal to that of the candidate profile, or less than ALTER and at the same time less than or equal to the most specific matching entry of the global access table, for example a member of the DATASET profile in class GLOBAL).

The *access list* and *conditional access list* comparison considers the account group membership for user IDs in the list. That is, a user ID in the conditional list of a redundant profile might be missing from the conditional access list of the candidate profile only, if one of the connect groups is present with the same access (and the same program name), and no connect groups are present with a higher access (and the same program name).

TheYou can access the command generation function fom option **RA.3.3** or by issuing the following command:

```
REMOVE REDUNDANT
```

Optionally, the number of profiles processed can be limited to a group of data sets by means of SELECT commands, `SELECT QUAL=id` for example.

For information about the method for showing non-redundant profiles and the reason they are non-redundant, see “RA.3.2 Non redundant - Data set profiles different from less specific profiles” on page 201.

Note: The redundancy check does not take all fields into account. For example, the RESOWNER and NOTIFY fields, and security categories, levels, and labels are not checked.

Finding inconsistencies in started task definitions

Started tasks are initiated by the `START` operator command, specified with an optional `SUB=` parameter to indicate a target subsystem. The default subsystem is the primary subsystem, usually JES2 or JES3. Security zSecure supports both JES2 and JES3 as the primary subsystem. It also supports the MSTR subsystem that is present in every MVS system.

When a started task is initiated, RACF first looks for a profile in the STARTED class with the format *procedure.jobname* to determine the user or group identity to assign to the task. If there is no such profile, or the profile does not contain an STDATA segment or STUSER specification, RACF falls back on the Started Procedure Table (ICHRIN03) to look for a match. You can use the STARTED and STCTABLE reports to review the contents of the STARTED class and the Started Procedure Table. See "STCTABLE - Started Procedure Table and Started Class" on page 288. To see the identities assigned to the started tasks, see "STCPROT - Started Task protection report" on page 344.

You can verify the consistency of the three information sources (ICHRIN03, RACF database, and procedure libraries) by issuing the **VERIFY STC** command.

The results of this function are only reliable when you supply a CKFREEZE file that was produced by running zSecure Collect from an authorized library. If you do not follow this requirement, STARTED profiles and ICHRIN03 entries can be incorrectly flagged as unused.

Be cautious about running the commands generated by the RDELETE command. If zSecure Collect is run with APF authorization, the program searches across memory functions to find the data sets allocated to STCPROC, or PROC00 if STCPROC is not available. Subsequently, it reads the PDS directory of each of these procedure libraries. It is insufficient to tell zSecure Collect to dump the directories of the PDS data sets in an unauthorized run because they are not recognized as procedure libraries.

For the STARTED class, the program checks for the following problems or inconsistencies:

1. Inactive classes that contain profiles that were never used.
2. Classes with profiles that do not cover any started task, as determined from the supplied CKFREEZE files.
3. Started tasks not covered by any profile that cause RACF to fall back to ICHRIN03 which is not advisable.
4. Profiles that do not have an STDATA segment.

   ICHRIN03 is used instead.
5. Profiles that do not have an STUSER specification in the STDATA segment.

   ICHRIN03 is used instead.
6. Profiles that have an STUSER specification that is not a valid RACF user ID.

   The JES undefined user is used instead.
7. Profiles that have an STGROUP specification that is not a valid RACF group ID.

   The JES undefined user is used instead.
8. Profiles that have valid user and group specifications that are not connected.

   The JES undefined user is used instead.
9. Profiles that specify a revoked user.

   This causes the started task to run with reduced authority, which might cause problems.

The verification function checks for these problems and issues commands to fix them if possible. The checks are performed based on the following processing rules:

- If the STARTED class is inactive, checks 2 through 9 are not performed.
- Checks 4 through 9 are only performed for profiles covering started tasks.

- If you are not interested in checks 6 on page 368 though 8 on page 368, add a SUPPRESS ID=++++++++ statement to the input commands. The checks are still done, but no commands are issued to fix any problems found. Also, if these checks fail, a further failure on check 9 on page 368 is not reported.

  Note: If you have changed the JES undefined user from ++++++++ to something else, specify the actual value on the suppress statement. This value is reported in the SETROPTS report in "SETROPTS - RACF settings report" on page 266 under the heading "Job Entry Subsystem options" as "Default uid local UNDEFINEDU". This value is also available in the UNDEFINEDUSER field of a SYSTEM NEWLIST .

For both the STUSER and STGROUP, the specification =MEMBER can be used instead of an explicit RACF user ID or group ID. This means that the member name of the started task being initiated is substituted for STUSER and STGROUP and matches a valid RACF user ID or group ID. (Obviously, this can never hold for both STUSER and STGROUP at the same time). As a result, some problems can be detected by simply looking at the STARTED profile (either does not contain =MEMBER, or has a discrete first qualifier which unambiguously identifies the substitution, or contains =MEMBER twice). Other problems require the evaluation of the member name and can only be detected on the started task level. For errors on the profile level, the program issues a single message for it. For some errors, the program might generate a command to try to fix the problem. For errors on the member level, the program issues a message on the member level, which can amount to several messages for a single profile. The program does not attempt to identify a fix for the error.

If more than one problem is detected, and the problems are of the same importance, they are both reported. However, if both a profile level problem and a member level problem are detected, only the profile level problem is reported. Therefore, after correcting the profile problems identified in the report, run the report again to identify any member level problems that might have been hidden in the initial report.

The following fixes can be generated to prevent profile errors:

- RDELETE is generated for an unused profile.
- For a profile without an STDATA segment, an STDATA segment with STUSER specification is created.
- Invalid STUSER or STGROUP specifications are deleted or replaced by =MEMBER if the specifications are clearly invalid.
- If =MEMBER is specified twice with a generic first qualifier, the STGROUP specification is deleted as this is the only solution that produces a usable profile.

The program does not generate any commands to address the following issues:

- Missing STUSER specification.
- Missing connection.
- Revoked user ID.
- Member level problems

If the STUSER specification is missing, the program purposely falls back to the Started Procedure Table ICHR1N03 which is the known solution for this problem. For the other problems, commands are not generated because the program cannot automatically determine what action or change is required to fix the problem.

For the Started Procedure Table ICHRIN03, the program checks for the following problems or inconsistencies:

1. Entries that do not cover any started task.

   This condition might be acceptable as a fallback when the STARTED class is inactive.
2. Started tasks that are not covered by any entry.

   These tasks are run with the default RACF user '*' , so this condition might not require a fix.
3. Generic entries that are not the last entry.

   These entries are not used.
4. Generic entries with a blank group name.

   If these entries exist, any user that can define started tasks can masquerade as any user.
5. Generic entries with the privileged or trusted attribute
6. Entries with a user specification that is not a valid RACF user ID.

   For these entries, the default RACF user '*' is used.
7. Entries with a group specification that is not a valid RACF group ID.

   For these entries, the default RACF user '*' is used.
8. Entries that have valid user and group specifications that are not connected.

   For these entries, the default RACF user '*' is used.
9. Entries that specify a revoked user.

   If the user has been revoked, the specified procedure cannot be started.
10. Entries with a valid user and group that have a revoked connect.

    If the connect has been revoked, the specified procedure cannot be started.

ICHRIN03 entries are even checked when they do not cover any started task because there are no matching tasks or because the tasks that match use a STARTED class profile instead. You can specify the SUPPRESS FALLBACK option, in which case only those entries that are currently in use are thoroughly checked for referential integrity and other problems. If this option is enabled, unused entries are still flagged. You might not want to use the suppress option if you want to check Fallback entries that are important because they are used to IPL the system when the STARTED class is inactive.

Figure 257 on page 371 shows relevant parts of the data from the VERIFY STC function. A CKFREEZE file is required for this function.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD070525.CKFREEZE'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |VERIFY STC
End of  CKRCMDV  (include level 1)
------------------------------------------------------------------------------------------------------------------------------
 M E S S A G E S   V E R I F Y   S T C                25 Mar 2007 00:05                                          page 5

 CKR0326 00 Started task runs with default authority    STCG10   IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STCG11   IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC03    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC04    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC05    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC08    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC09    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC10    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC11    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC12    IPL130 SYS1.PROCLIB                                fallback
 CKR0326 00 Started task runs with default authority    STC01    IPL130 SYS1.PROCLIB                                system
 CKR0326 00 Started task runs with default authority    STC02    IPL130 SYS1.PROCLIB                                system
 CKR0326 00 Started task runs with default authority    STC06    IPL130 SYS1.PROCLIB                                system
 CKR0326 00 Started task runs with default authority    STC07    IPL130 SYS1.PROCLIB                                system
 CKR0563 08 STARTED profile STC07.STC07 has no STDATA segment - ICHRIN03 will be used - change to NOUSER
 CKR0576 00 No STARTED profile found, ICHRIN03 will be used - STC01    IPL130 SYS1.PROCLIB
 CKR0577 00 STARTED profile STC13.STC13 not used by any started procedure
 CKR0566 08 STARTED profile STC04.STC04 has undefined STUSER STC04 - "++++++++" will be used -
            change to NOUSER
 CKR0566 08 STARTED profile STC11.STC11 has undefined STUSER STC11 - "++++++++" will be used -
            change to NOUSER
 CKR0568 08 STARTED profile STCG1*.* has STUSER =MEMBER, which is undefined - "++++++++" will be used for STCG11   IPL130 SYS1.PROCL
 CKR0565 08 STARTED profile STC05.STC05 contains group id SYS1 as STUSER - "++++++++" will be used -
            change to NOUSER
 CKR0571 08 STARTED profile STC12.STC12 has undefined STGROUP STC12 - "++++++++" will be used -
            correct to NOGROUP                      but userid still revoked
 CKR0575 08 STARTED profile STC10.STC10 has revoked userid STC10 - will execute with reduced access
 CKR0574 08 STARTED profile STC08.STC08 user STRTASK not connected to group STC06 - "++++++++" will be used
 CKR0564 08 No STUSER specified on STARTED profile STC02.STC02 - ICHRIN03 will be used
```

Figure 257. Sample VERIFY STC output

If the (possibly many) messages CKR0326 are not required, they can be suppressed by SUPPRESS MSG=326. The same holds for messages 576 and 577; recall in the case of CKR0577, however, that suppressing a message will not suppress the associated command (RDELETE in this case).

The generated commands look like the commands in the following figure.

```
  File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       C##BJTI.C2R1EF2A.CKRCMD                       Columns 00001 00072
Command ===>                                               Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001         /* CKRCMD file CKR1CMD complex VERI#STC NJE OS390R3 generated 10
000002          /* Commands generated by VERIFY STC        */
000003         ralter started STC07.STC07 stdata(NOUSER)
000004         rdelete started STC13.STC13
000005         ralter started STC04.STC04 stdata(NOUSER)
000006         ralter started STC11.STC11 stdata(NOUSER)
000007         ralter started STC05.STC05 stdata(NOUSER)
000008         ralter started STC12.STC12 stdata(NOGROUP)
000009         SETROPTS REFRESH RACLIST(STARTED) /* POSIT 66 */
****** **************************** Bottom of Data ****************************
```

Auditing CKGRACF

You can audit the use of CKGRACF using the following CKGRACF features.

- The SHOW CKRSITE command displays the installation-defined settings stored in the CKRSITE module. For details, see "The CKRSITE module" on page 372.
- After a CKGRACF command completes, a RACF SMF record (SMF 80, EVENT=GENERAL) is written which records information about the command and its effects. For details, see "RACF processing records" on page 373.

- If CKGRACF profiles are being audited, each RACF logging record for these profiles (SMF 80, EVENT=ACCESS) contains a description of the command being executed and the CKGRACF application name. For details, see “RACF processing records” on page 373.
- All CKGRACF settings in user profiles contain a stamp with the command-issuing user and the date and time the command was executed. This stamp is displayed with the LIST USER command and in the USR field in Security zSecure. For details, see “CKGRACF settings in the user profile” on page 376.
- Completed queued commands and wiped scheduled actions are not deleted immediately, but remain in the user profile until an installation-defined auditing period has passed. For details, see “CKGRACF settings in the user profile” on page 376.

Note that Security zSecure also provides support to audit CKGRACF. For example, the REPORT SCOPE command reports the users and groups within the CKGRACF-defined scope. For details, see “REPORT” on page 875

The CKRSITE module

The optional CKRSITE module contains the installation-defined settings for CKGRACF. These settings can be displayed using the SHOW CKRSITE command, which results in output like in Figure 258.

```
CKGRACF SHOW CKRSITE
CKG100I 00 Contents of CKRSITE module:
           Class:              XFACILIT
           Authority:          SINGLE
           Command expiration: 7
           Audit expiration:   30
```

Figure 258. Sample output of the SHOW CKRSITE command

The meaning of the listed settings is:

- The class checked for CKGRACF profiles is XFACILIT. Thus, when the manual refers to 'command resource name CKG.CMD.REFRESH', the XFACILIT class is checked for a profile matching that resource name.
- The default multiple-authority setting is SINGLE. This means that any user without a multiple-authority requirement of its own, is subject to single authority. Other options are DUAL and TRIPLE.
- The command expiration time is 7 days. This means that a queued command must be acted upon within 7 days of the last action. After 7 days, the queued command expires and can no longer be executed.
- The Audit expiration time is 30 days. This means that completed or expired commands, and ineffective or wiped scheduled actions are deleted after 30 days. Until that time, the completed commands and wiped scheduled actions can be displayed using the LIST USER command.

You should verify that these options are the same in the CKRCARLA program. The Security zSecure command SHOW CKRSITE can be used to display those settings.

RACF processing records

Background

At the end of each CKGRACF command, a RACF processing record (SMF 80) is written with EVENT=GENERAL. The EVENT=GENERAL record contains the following fields of interest:

- The DESCRIPTOR field (SMF80DES) indicates whether the command succeeded or failed. (The RACF report writer RACFRW describes this as VIOLATIONS and SUCCESSES.)
- The LOGSTR field contains the CKGRACF command and always starts with the word *CKGRACF*. The log string never contains sensitive data like passwords. You can select records with a log string of this format with the option LOGSTR=:CKGRACF. The RACF Report Writer (RACFRW) describes this field as LOGSTR.

  The log string in a RACF SMF record can have 255 characters at most. Some parts of CKGRACF commands with more than 255 characters are not logged because they exceed this length. The length is typically exceeded on commands that have very long REASON strings. Devising a shorterREASON string can prevent commands from being omitted from the logs.
- The USER and GROUP fields–*SMF80USR* and *SMF80GRP*, for example, contain the name of user who issued the command along with the current connect group for that user.
- The CLASS and PROFILE fields contain the class and profile name of the target profile. For example, a CKGRACF USER command has CLASS set to USER and PROFILE set to the target userid. This feature is only available with zSecure Audit for ACF2, not with the RACFRW.

If the CKGRACF profiles are being audited, RACF processing records (SMF 80) are written with EVENT=ACCESS. When access violations are selected, all failed access checks are found; when access successes are selected, all successful access checks are found. However, in those cases where CKGRACF permits access because one profile out of several granted access based on the USR scope check for example, a success is logged on the first profile granting access or failure is logged on all profiles that denied access. Consequently, if the third step in the USR scope check grants access, failures are not logged for the first two steps in the scope check.

A profile can be audited using the RALTER GLOBALAUDIT command. For example, to audit access failures to the profile CKG.CMD.AUTHORITY, and successful access to the profile CKG.CMD.RDELETE, use the following commands:

```
RALTER XFACILIT CKG.CMD.AUTHORITY GLOBALAUDIT(FAILURES(READ))
RALTER XFACILIT CKG.CMD.RDELETE GLOBALAUDIT(SUCCESS(READ))
```

See the 'Security Server RACF Auditor's Guide' and the 'Security Server RACF Command Language Reference' for more details.

The EVENT=ACCESS record contains the following fields of interest:

- The DESCRIPTOR field (SMF80DES) indicates whether the command succeeded or failed. (The RACFRW describes this as VIOLATIONS and SUCCESSES.)
- The LOGSTR field usually contains the command string which always starts with the word CKGRACF. (The log string never contains sensitive data such as passwords.) Selecting the records with a log string of this format can be done using LOGSTR=:CKGRACF. (The RACFRW describes this field as LOGSTR.) Incidentally, the log string can be missing from a RACF record written by

CKGRACF with EVENT=ACCESS. RACF records written by CKGRACF with EVENT=ACCESS can be selected regardless of a missing LOGSTR using LOGSTR=:CKGRACF,OR,APPL=CKGRACF.

- The USER and GROUP fields (SMF80USR and SMF80GRP) contain the name of the command-issuing user and his or her current connect group.
- The EVENTQUAL field (SMF80EVQ) contains the numerical event qualifier, which describes the kind of access event. (The RACFRW describes this field as EVQUAL.)
- The RESOURCE field contains the resource name checked. (The RACFRW describes this field as NAME or RESOURCE.)
- The PROFILE field contains the profile checked. In the case of a discrete profile, this is identical to RESOURCE; in the case of a generic profile, this is the real profile checked. (This field is not listed by the RACFRW.)
- The ACCESS and INTENT fields contain the intended and permitted access.

Auditing RACF processing records

To audit the use of CKGRACF profiles and commands, the standard query "CKGRACF" is available under menu option **EV.2**. Select that query, and complete the selection criteria in the next panel, then press enter to start the query. A sample display is shown in the following figure.

```
SMF record RACF processing and audit records                  Line 145 of 1300
Command ===> _____________________________________________ Scroll===> CSR
                                          4Sep00 08:26 to 10Sep00 00:17

   Date      Time  Description
__ 05Sep2000 00:46 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:46 RACF CKG success for C##QAP1: logstr=CKGRACF SHOW MYACCESS
__ 05Sep2000 00:49 RACF ACCESS success for C##QAP1: (UPDATE,UPDATE) on FACILITY
__ 05Sep2000 00:49 RACF ACCESS success for C##QAP1: (UPDATE,UPDATE) on FACILITY
__ 05Sep2000 00:49 RACF ACCESS success for C##QAP1: (UPDATE,UPDATE) on FACILITY
__ 05Sep2000 00:49 RACF ACCESS violation for C##QAP1: (UPDATE,NONE) on FACILITY
__ 05Sep2000 00:49 RACF ACCESS violation for C##QAP1: (UPDATE,NONE) on FACILITY
s_ 05Sep2000 00:49 RACF CKG violation for C##QAP1: logstr=CKGRACF USER ADM1 PWS
__ 05Sep2000 00:49 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:49 RACF CKG success for C##QAP1: logstr=CKGRACF SHOW MYACCESS
__ 05Sep2000 00:51 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:51 RACF CKG success for C##QAP1: logstr=CKGRACF SHOW MYACCESS
__ 05Sep2000 00:52 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:52 RACF CKG success for C##QAP1: logstr=CKGRACF ACCESS C##BMR1
__ 05Sep2000 00:54 RACF ACCESS success for C##QAP1: (UPDATE,UPDATE) on FACILITY
__ 05Sep2000 00:54 RACF CKG violation for C##QAP1: logstr=CKGRACF CMD AT 05Sep2
__ 05Sep2000 00:54 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:54 RACF CKG success for C##QAP1: logstr=CKGRACF SHOW MYACCESS
__ 05Sep2000 00:56 RACF ACCESS success for C##QAP1: (READ,READ) on FACILITY $CN
__ 05Sep2000 00:56 RACF CKG success for C##QAP1: logstr=CKGRACF ACCESS C##B DAT
__ 05Sep2000 00:56 RACF ACCESS violation for C##QAP1: (UPDATE,NONE) on FACILITY
__ 05Sep2000 00:56 RACF CKG violation for C##QAP1: logstr=CKGRACF AUTHORITY GRO
```

The records with a description starting with "RACF CKG" log CKGRACF commands, while the "RACF ACCESS" records document checks against CKGRACF profiles. A sample CKGRACF command log record is shown in the following figure.

```
SMF record RACF processing and audit records                    Line 1 of 37
Command ===> ____________________________________________ Scroll===> CSR
                                          2May01 13:54 to  4May01 16:44

  Description
  RACF CKG violation for C##QAP1: logstr=CKGRACF ADM1 PWSET PASSWORD(********)

  Record identification
_ Jobname + id:  CRMCWGS
  SMF date/time: Wed  2 Mar 2001 13:54:37.64
  SMF system:    DINO       record type:  80   record no: CNR5SM00 409617

  Event identification
  RACF event description        General auditing (Unclear:General audit record
  RACF event description        written)
  RACF event qualifier          0
  RACF descriptor for event     Violation
  RACF reason for logging
  SAF authority used
  Unix Audit Function Code
  Access intent
  Access allowed
  Audit/message logstring       CKGRACF ADM1 PWSET PASSWORD(********)

  Object identification
  SAF profile class             USER
_ SAF profile key               ADM1
_ SAF resource name             ADM1
  Resource level                 0
  Volume serial
  Resource token

  Object ownership
  Profile owner id
  Installation data

  Subject identification
_ User:  C##QAP1      Group: C##QA        Terminal:            Appl:
  Name:  GRPSPEC RACFWIN USER             Security label:
  Token: User:C##QAP1; Group:C##QA; Session:OMVSSRV
****************************** BOTTOM OF DATA ********************************
```

Violations are recorded in the log record as shown in the following example:

```
User C##QAP1 was not permitted to set the password for user ADM1.
```

In the log record, the requested password is replaced by asterisks. If the class configured in the CKRSITE module has the proper logging for RACF, an access violation is also written showing the profile that prevented access.

In this particular case, the preceding record shows a failed CKGRACF profile check as shown in Figure 259 on page 376: User *ADM1* is not in the ID-scope of *C##QAP1* and the id-hierarchical (SCP.G/U) scope check also failed, so the CKGRACF command is refused. See "Scope profiles" on page 1563 for a detailed explanation.

```
SMF record RACF processing and audit records                    Line 1 of 36
Command ===> _____________________________________________ Scroll===> CSR
                                          2May01 13:54 to  4May01 16:44


  Description
  RACF ACCESS violation for C##QAP1: (UPDATE,NONE) on FACILITY
  $CNG.SCP.ID.ADM1.ADMIN.ADMIN

  Record identification
_ Jobname + id:  C##QAP1
  SMF date/time: Wed  2 Mar 2001 13:54:37.64
  SMF system:    DINO       record type:  80   record no: CNR5SM00 409614

  Event identification
  RACF event description        Resource access (Failure:Insufficient
  RACF event description        authority)
  RACF event qualifier          1
  RACF descriptor for event     Violation
  RACF reason for logging       Resource Logoptions
  SAF authority used            Normal
  Access intent                 UPDATE
  Access allowed                NONE
  Audit/message logstring       CKGRACF ADM1 PWSET PASSWORD(********)

  Object identification
  SAF profile class             FACILITY
  SAF profile key               $CNG.SCP.ID.ADM1.ADMIN.ADMIN
_ SAF resource name             $CNG.SCP.ID.ADM1.ADMIN.ADMIN
  Resource level                 0
  Volume serial
  Resource token

  Object ownership
_ Profile owner id              SYSAUTH
  Installation data             AUTHORIZATION GROUPS

  Subject identification
_ User:  C##QAP1      Group: C##QA        Terminal:            Appl:
  Name:  GRPSPEC RACFWIN USER             Security label:
  Token: User:C##QAP1; Group:C##QA; Session:OMVSSRV
******************************* BOTTOM OF DATA ********************************
```

Figure 259. SMF record RACF processing and audit records panel

CKGRACF settings in the user profile

All CKGRACF settings in the user profile contain a stamp with the command-issuing user and the date and time the command was executed. The settings and the stamp can be displayed using the CKGRACF LIST command. The LIST command displays the following types of information:

- Multiple-authority settings.
- The availability of a default password.
- All scheduled revoke/resume events.
- All queued commands.

All completed queued commands and past scheduled revoke/resume settings that lie within the installation-defined auditing period are kept in the user profile and are also displayed. Figure 260 on page 377 shows sample output of the LIST USER command; note that withdrawn queued commands and deleted scheduled actions are also listed.

```
CKGRACF LIST USER C##CX02

------------ Status of USER C##CX02 on 10Nov1999 17:17 at DINO -------------
---------------------------- Revoked PwdExpired -----------------------------
Last use date:     05Oct1999 00:00:00.00
Last connect date: 11Mar1999 09:52:33.31

Username             RI SOA AG Created   PwChanged/Int/Try Owner    Dfltgrp
TEST USER, NO TSO    R- --- -- 02Feb1996 Expired    30   0 C##C     C##C

Groupname Auth R SOA AG T Uacc Connected Instdata
>C##C     USE  - --- -- - NONE 02Feb1996 EXTERNE GEBRUIKERS

CKG132I 00 No CKGRACF queued command entries found
CKG116I 00 Scheduled revoke for $DELETE on 25Oct1999 by C##QARUN 25Oct1999 14:08
           Reason: LUKT TOCH NIET
CKG117I 00 --- Overall revoke/resume status ---
           Revoked from 25 Oct 1999
```

Figure 260. Sample output of the LIST USER command

Security zSecure can also be used to list a user profile's USR fields. By default, the USR field lists both the CKGRACF-RESERVED entries and the installation-defined entries, as shown by the sample output in Figure 261.

```
zSecure Suite User Defined Display                          Line 1 of 10
Command ===>                                               Scroll===> PAGE
                                                 4 Mar 1994 17:13
  CKGRACF data
  Authority setting DUAL set by R#OPADM at 28 Feb 1994 20:00
_ Queued command (R): USER C##CX02 SCHEDULE ZSECUR99 DISABLE (10Dec1994:14Dec19
_ Queued command (R): USER C##CX02 SCHEDULE ZSECUR99 DISABLE (01Jul1994:15Jul19
_ Queued command (R): USER C##CX02 SCHEDULE ZSECUR99 DISABLE (10Mar1994:01Apr19
_ Queued command (R): USER C##CX02 PWDEFAULT PASSWORD; request by C##AROB at  4
_ Queued command (W): USER C##CX02 RESUME; request by C##AROB at  4 Mar 1994 15
****************************** BOTTOM OF DATA ********************************
```

Figure 261. Sample Security zSecure detail display of the USR field

As described in "RA.2 QUEUED - Queued commands" on page 185, line commands can be used to approve, hold, or deny queued commands, and to copy or add new queued commands, schedules, and installation-defined USR entries.

Predefined CARLa scripts

In this section, the ISPF and batch sample reports available in the SCKRCARL library are discussed. The convention used to name CARLa scripts members is explained in "Naming convention" on page 706.

Interactive reports

The following interactive (ISPF) RACF reports are available.

Table 187. Interactive RACF reports

Report	Meaning
CKAD@CO	Audit concerns for RACF control for creating the audit concern overview.
CKAD@RO	Audit concerns for resource protection (used to build audit concern overview)
CKADRFIL	Show sensitive UNIX files. Automatically included by CKRDAC1.
CKADRFW	Show globally writable UNIX files. Automatically included by CKRDRGBW.

Table 187. Interactive RACF reports (continued)

Report	Meaning
CKADRPAU	RACF profile audit concerns.
CKADRTRU	Show sensitive resources with trustees
CKADRUGD	Show UNIX UIDs and GIDs, used somewhere in a UNIX file system but not defined to RACF.
CKADSD80	Audit concerns for RACF SETROPTS settings (80 characters wide). Automatically included by CKRDSD80.
CKADSR80	Audit concerns for RACF settings and options. Automatically included by CKRDSR80.
CKADUTRU	Show trusted users.
CKRDAC1	Protection of APF modules (REPORT AC1). Automatically includes CKADRFIL.
CKRDAUTH	Authorized user (Special, Operations, Auditor) report. This also shows the class authorizations, and users with uid 0.
CKRDCLAS	Class Descriptor Table, SETROPTS settings, and RACF profiles report.
CKRDDCLS	RACF class info from database ICB
CKRDENT#	Entity and segment summary.
CKRDGAU	Group-authorized user report.
CKRDGLOB	Global Access Table overview.
CKRDLGAD	Overview of user by last logon date, detailed report.
CKRDLGAG	Overview of last logon ages, summary only.
CKRDLGER	Overview of users with logon failures (detailed).
CKRDLGE0	Over of users with logon failures (concise).
CKRDLGNU	Overview of users that have never been used.
CKRDLGRV	Userids with pending revoke due to inactivity.
CKRDOMVS	Show users with duplicate UIDs and groups with duplicate GIDs
CKRDPADS	Program Access to Data Sets (REPORT PADS).
CKRDPWAD	Overview of password ages, detailed report.
CKRDPWAG	Overview of password ages, summary only.
CKRDPWIN	Overview of users with exceptional password interval.
CKRDPWNU	Overview of users with initial passwords.
CKRDPWXP	User IDs with expired passwords.
CKRDRGBW	Show global write access. Automatically includes CKADRFW.
CKRDRROV	Summary table of general resource profiles.
CKRDSAUT	RACF Authorized Caller Table.
CKRDSD80	RACF SETROPTS settings in database. Automatically includes CKADSD80.
CKRDSDSN	RACF Data Set Name Table.
CKRDSENP	Profiles covering sensitive data (REPORT SENSITIVE)
CKRDSPT	RACF Started Procedures Table and STARTED class.
CKRDSRFR	SAF Router Table.

Table 187. Interactive RACF reports (continued)

Report	Meaning
CKRDSRNG	RACF Data Set Range Table.
CKRDSR80	RACF settings and options. Automatically includes CKADSR80.
CKRDSTC	Protection of started tasks (REPORT STC).
CKRDTEMP	RACF template display (with detail selection)
CKRDTEM0	RACF template display (no detail selection)
CKRD2DIF	Compare profile existence in 2 RACF databases (edit data set names first)

Batch reports

The following batch RACF reports are available (these start with CK%L or CKRR). The CKRR* members are the original (backward compatibility) layouts for a number of REPORT command parameters.

Table 188. CARLa scripts - Batch reports

Report	Meaning
CKAL$ALL	Collection of all system and many RACF-specific reports
CKAL$CD	Collection of reports on RACF control
CKAL$RD	Collection of reports on resources for RACF
CKAL$UD	Collection of reports on RACF users
CKAL@ALL	Overview of audit concerns from all system and many RACF-specific reports
CKAL@CO	Audit concerns for RACF control (used to build audit concern overview)
CKAL@RO	Audit concerns for resource protection with RACF (used to build audit concern overview)
CKALRFIL	Show sensitive UNIX files. Automatically included by CKRLAC1.
CKALRFW	Show globally writable UNIX files. Automatically included by CKRLRGBW.
CKALRPAU	RACF profile audit concerns.
CKALRTRU	Show sensitive resources with trustees.
CKALRTR0	Show sensitive resources (concise).
CKALRUGD	Show UNIX UIDs and GIDs, used somewhere in a UNIX file system but not defined to RACF.
CKALSD13	Audit concerns for RACF SETROPTS settings (132 characters wide). Automatically included by CKRLSD13.
CKALSD80	Audit concerns for RACF SETROPTS settings (80 characters wide). Automatically included by CKRLSD80.
CKALSR13	Audit concerns for RACF settings and options (132 characters wide). Automatically included by CKRLSR13.
CKALSR80	Audit concerns for RACF settings and options (80 characters wide). Automatically included by CKRLSR80.
CKALUTRU	Show trusted users (detailed).
CKALUTR0	Show trusted users (concise).

Table 188. CARLa scripts - Batch reports (continued)

Report	Meaning
CKRL$ALL	Collection of RACF reports.
CKRLAC1	Protection of APF modules (REPORT AC1). Automatically includes CKALRFIL.
CKRLAPPL	Overview of APPL application profiles.
CKRLAUD	Show non-default auditing parameters (audited users, success audit, non-default failure audit).
CKRLAUTH	Authorized user (Special, Operations, Auditor) report, including class authorizations, and uid 0.
CKRLCICS	Resolved access list of all CICS-related profiles.
CKRLCICT	Resolved CICS transaction authorization report (combines members of grouping profiles with member profiles)
CKRLCLAS	Overview of CDT and SETROPTS settings.
CKRLCLS#	Class info for classes with one or more profiles.
CKRLDB2	Overview of DB2-related profiles, and users with CICS, DDF, or IMS access to DB2®.
CKRLDCLS	RACF class info from database ICB
CKRLENT#	Entity and segment summary.
CKRLGAU	Group-authorized user report.
CKRLGLOB	Global Access Table overview.
CKRLGRPI	Two-pass query to show group tree with added user information, to aid in designing administration authorities.
CKRLGRPT	Group-tree overview.
CKRLIMS	Overview of IMS-related profiles.
CKRLINAC	Overview of inactive users.
CKRLJES2	Overview of JES2-related profiles.
CKRLLGAD	Overview of last logon date, detailed report.
CKRLLGAG	Overview of last logon date, summary only.
CKRLLGER	Overview of users with logon failures.
CKRLLGNU	Overview of users that have never been used.
CKRLLGRV	Show user IDs with pending revoke due to inactivity.
CKRLMTX1	Two-pass query to show a data set access matrix for selected users (customization is necessary).
CKRLMTX2	Two-pass query to show a connection matrix for selected `userids` and groups (customization is necessary).
CKRLMTX3	Query to obtain a matrix of userids with access to selected data set profiles (imbed member after RACFSEL selection NEWLIST; see member for an example).
CKRLOMVS	Show users with duplicate UIDs and groups with duplicate GIDs.
CKRLPADS	Program Access to Data Sets (REPORT PADS).
CKRLPROG	Program profile and PADS overview.
CKRLPWAD	Overview of password age, detailed report.
CKRLPWAG	Overview of password age, summary only.

Table 188. CARLa scripts - Batch reports (continued)

Report	Meaning
CKRLPWIN	Overview of users with exceptional password interval.
CKRLPWNU	Overview of users with initial passwords.
CKRLPWXP	Show `userids` with expired passwords.
CKRLREV	Overview of revoked users and (non-RDS only) revoked connects.
CKRLRGBW	Show global write access. Automatically includes CKALRFW.
CKRLSAUT	RACF Authorized Caller Table.
CKRLSCPS	Two-pass query to show scope reports for more than one user.
CKRLSD13	RACF SETROPTS settings in database (132 column display). Automatically includes CKALSD13.
CKRLSD80	RACF SETROPTS settings in database (80 column display). Automatically includes CKALSD80.
CKRLSDSF	Overview of SDSF-related profiles.
CKRLSDSN	RACF Data Set Name Table.
CKRLSENP	Profiles covering sensitive data (REPORT SENSITIVE).
CKRLSPT	Started Procedure Table and STARTED profiles.
CKRLSRFR	SAF Router Table.
CKRLSRNG	RACF Data Set Range Table.
CKRLSR13	RACF settings and options (132 column display). Automatically includes CKALSR13.
CKRLSR80	RACF settings and options (80 column display). Automatically includes CKALSR80.
CKRLSTC	Protection of started tasks (REPORT STC).
CKRLTAPE	Overview of TAPEVOL profiles.
CKRLTEMP	Template display (used by SHOW TEMPLATE).
CKRLUNAM	Overview of user names and installation data.
CKRLVHL	Userids and groups for which no high level (catchall) profile was found.
CKRLVSTD	Verify that the owner of a data set profile is the high-level qualifier.
CKRLVSTG	Verify that the owner of a group is the superior group.
CKRLVSTU	Verify that the owner of a user is the default group.
CKRRAC1	REPORT AC1 default layout (used if no NEWLIST TYPE=REPORT_AC1 was specified)
CKRRPADS	REPORT PADS default layout (used if no NEWLIST TYPE=REPORT_PADS was specified)
CKRRSENS	REPORT SENSITIVE default layout (used if no NEWLIST TYPE=REPORT_SENSITIVE was specified)
CKRRSTC	REPORT STC default layout (used if no NEWLIST TYPE=REPORT_STC was specified)
CKRVTCB	List and check protection of Trusted Computing Base

Table 188. CARLa scripts - Batch reports (continued)

Report	Meaning
CKRVWORM	Report globally writable resources. Globally writable data sets can be used to install trojan horses.
C2RL$UNL	Create RACF and ACF2 unload and report statistics

We advise you to run the overall report, CKRL$ALL, at least once. You are then able to decide which reports are useful at your installation, and which sample reports must be edited.

Chapter 4. Resource reports

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The **RE Resource reports** option available on the zSecure Audit Main menu shown in Figure 262 provides access to display and reporting options for RACF resources. You can access additional display and reporting options from the Audit Status (**AU.S**) option available on the Audit menu as described in Chapter 3, "RACF Audit Guide," on page 255.

Note: The Main menu is available from the interactive ISPF application available under both MVS/TSO and VM/CMS. For instructions on starting this application, see "Starting the interactive component" on page 9. For information about panel structure and operation, see "Panel structure" on page 10. For information about any of the fields on any of the zSecure panels, use the field-sensitive help function.

```
 Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                        zSecure Admin+Audit for RACF - Main menu
Option  ===> ____________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
RE   Resource        Resource reports
       I IP Stack      TCP/IP stack reports
       U Unix          Unix filesystem reports
       C CICS          CICS region and resource reports
       M IMS           IMS control region and resource reports
       D DB2           DB2 region report
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex: DAILY
```

Figure 262. zSecure Audit for RACF Main menu

The Resource reporting options provide access to reports about the IP stack configuration and statistics, UNIX file system, auditing functions for TCP/IP, and auditing functions for CICS, IMS, and DB2. For more information about the Resource menu options, see the sections indicated in Table 189.

Table 189. Documentation reference for zSecure Menu options

Menu Option	Documentation reference
I IP Stack	"IP Stack reports" on page 384
U Unix filesystem reports	"UNIX filesystem reports (RE.U)" on page 390
C CICS region and resource reports	"CICS resource reports" on page 402
M IMS control region and resource reports	"IMS resource reports" on page 413

Table 189. Documentation reference for zSecure Menu options (continued)

Menu Option	Documentation reference
D DB2 region report	"DB2 resource reports" on page 422

IP Stack reports

The RE.I option can be used to select and display TCP/IP stack configuration data. This data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized with the `TCPIP=YES` parameter.

When you select RE.I from the main menu, the panel shown in Figure 263 is displayed.

```
 Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Resource - IP stack Selection
Command ===> ____________________________________________________   _ start panel

Show TCP/IP stack configuration data that fit all of the following criteria:
Stack name . . . . . ________ (name or filter)
System . . . . . ________ (system or filter)
Sysplex  . . . . . ________ (sysplex or filter)

Output/run options
_  Ports                  _  Rules                  _  VIPA
_  Interfaces             _  Routes                 _  Netaccess
_  AUTOLOG                _  Resolver
_  Output in print format  _  Customize title       _  Send as e-mail
  _  Run in background
```

Figure 263. IP stack Selection panel

From the IP stack Selection panel, you can limit the TCP/IP stack configuration data by entering selection criteria into one or more fields. When you specify selection criteria, only records that match all criteria are included in the output. Filters can be used in some of the selection fields. For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1).

You can also specify Output and run options on the Selection panel. The run options (Ports, Rules, VIPA, Interfaces, Routes, Netaccess, and AUTOLOG) allow you to specify additional selection criteria for specific types of IP configuration data. The output run options allow you to specify report and print options. When you select any of these options, the corresponding panels are displayed when you press Enter on the IP stack Selection panel.

If you do not select any Output or run options, the data is processed as soon as you press Enter on the IP Stack Selection panel. An overview panel is immediately displayed with a summary of the IP configuration records that match the selection criteria that you specified.

See the following topics for information about specifying configuration data, selection criteria, and report output options.

"IP stack configuration data: Viewing summary and detail information" on page 385

"IP stack port configuration data - Specifying selection criteria" on page 385

"IP stack rules configuration data - Specifying selection criteria" on page 386

IP stack configuration data: Viewing summary and detail information

After processing the CKFREEZE file, the TCP/IP stack configuration report selection panel is displayed. This panel is displayed immediately from the IP stack Selection panel if you have not selected any of the output or run options. If you have selected output or run options, this panel is displayed after you have entered the required data for the selected options. In Figure 264 the summary data for all IP stack configuration data is listed.

```
         zSecure Suite Display Selection 1 s elapsed, 0.6 s CPU
Command ===> ____________________________________________ Scroll===> PAGE

  Name     Summary Records Title
_ IPSTACK        1       1 Communications Server IP stack display
_ IPPORT         1      33 Communications Server IP ports display
_ IPRULE         1       2 Communications Server IP rules display
_ IPVIPA         0       0 Communications Server IP VIPA display
_ IPINTFD        1       4 Communications Server IP interfaces display
_ IPROUTE        1       4 Communications Server IP routes display
_ IPNETACC       0       0 Communications Server IP netaccess display
_ IPAUTOL        1       2 Communications Server IP autolog display
****************************** Bottom of Data ********************************
```

Figure 264. TCP/IP stack configuration report selection

In this example, the overview panel includes information for all of the IP configuration record types based on the selection criteria specified on the IP Stack Selection panel. Only records that match the specified the selection criteria are included.

To filter the summary results by configuration type, you can select a specific IP configuration record type on the Display Selection panel, IPAUTOLOG for example. When the report based on this selection is generated, the overview panel only shows a summary entry for the IPAUTOLOG. To see an overview of the records reported for each configuration type, select the summary line for that type.

From each overview panel, you can navigate to one or more detail panels by selecting a record entry.

For more information about the IP stack configuration reports, see "STATUS AUDIT - MVS tables" on page 440.

IP stack port configuration data - Specifying selection criteria

When you select the **Ports** option on the Resource - IP stack Selection panel (Figure 263 on page 384) opens the panel shown in Figure 265 on page 386 where

you can specify the port attributes you are interested in.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show ports that fit all of the following criteria:
Port number . . . . . ___________  (port number or range (e.g. 1000:2000))
Jobname . . . . . ________     (jobname or filter)
Bind IP address . . . . ________________________________________
SAF resource name . . . ________     (resource name or filter)
Protocol  . . . . . _  1. TCP      2. UDP      3. Both
```

Figure 265. IP stack - selection - ports

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPPORT - Communications Server IP ports display report" on page 490 for more information about the IP_PORT report.

IP stack rules configuration data - Specifying selection criteria

When you select the **Rules** option on the Resource - IP stack Selection panel (Figure 263 on page 384), the Figure 266 is displayed. On this panel, you can specify selection criteria for reporting on IP_RULE configuration data. When you run the report, the results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show rules that fit all of the following criteria:
Source IP address . . . ________________________________________
Source IP port  . . . . _____  (number or filter)
Destination IP address  ________________________________________
Destination IP port . . _____  (number or filter)
Protocol  . . . . . _  ICMP   _  TCP    _  UDP    _  ICMPV6 _  OSPF
Routing type  . . . . . _  1. Local    2. Routed   3. Either
```

Figure 266. IP stack - selection - rules

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPRULE - Communications Server IP rules display report" on page 492 for more information about the IP_RULE report.

IP stack VIPA configuration data - Specifying selection criteria

When you select the **VIPA** (Virtual IP address) option on the Resource - IP stack Selection panel (Figure 263 on page 384), the Figure 267 on page 387 is displayed. On this panel, you can specify selection criteria for reporting on IP_VIPA configuration data. When you run the report, the VIPA results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show VIPA addresses that fit all of the following criteria:
Virtual IP address  . . ____________________________________________
IPV6 interface name . . _______________  (name or filter)
VIPA type   . . . . . . _  1. Backup  2. Define  3. Range   4. All
```

Figure 267. IP stack - selection - VIPA

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPVIPA - Communications Server IP VIPA report" on page 492 for more information about the IP_VIPA report.

IP stack interface configuration data - Specifying selection criteria

When you select the **Interfaces** option on the Resource - IP stack Selection panel (Figure 263 on page 384), the panel shown in Figure 268 is displayed. On this panel, you can specify selection criteria for reporting on IP stack interfaces configuration data. When you run the report, the results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show interfaces that fit all of the following criteria:
Interface name  . . . . _______________  (name or filter)
IP address  . . . . . . ____________________________________________
Virtual LAN id  . . . . _______________  (id or filter)
```

Figure 268. IP stack - selection - interfaces

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPINTFD - Communications Server IP interfaces report" on page 493 for more information about the IP_INTERFACE report.

IP stack route configuration data - Specifying selection criteria

When you select the **Route** option on the Resource - IP stack Selection panel (Figure 263 on page 384), the Figure 269 on page 388 is displayed. On this panel, you can specify selection criteria for reporting on IP Route configuration data. When you run the report, the results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show routes that fit all of the following criteria:
Source IP address . . . ____________________________________________
Destination IP address  ____________________________________________
Interface name  . . . . ________________  (name or filter)
```

Figure 269. . IP stack - selection - routes

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPROUTE - Communications Server IP routes report" on page 494 for more information about the IP_ROUTE report.

IP stack network access configuration data - Specifying selection criteria

When you select the **Netaccess** option on the Resource - IP stack Selection panel (Figure 263 on page 384), the Figure 270 is displayed. On this panel, you can specify selection criteria for reporting on IP Network access configuration data. When you run the report, the results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Show netaccess data that fit all of the following criteria:
IP address  . . . . . . ____________________________________________
RACF profile name   . . ____________________________________________
SAF resource name   . . ________________  (resource name or filter)
Check requests  . . . . _  1. Inbound  2.  Outbound  3.  Both
```

Figure 270. IP stack - selection - netaccess

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPNETACC - Communications Server IP netaccess display report" on page 495 for more information about the IP_NETACC report.

IP stack AUTOLOG configuration data - Specifying selection criteria

When you select the **AUTOLOG** option on the Resource - IP stack Selection panel (Figure 263 on page 384), the Figure 271 on page 389 is displayed. On this panel, you can specify selection criteria for reporting on IP stack AUTOLOG configuration data. When you run the report, the results include only the records that match the selection criteria specified on the IP stack Selection panel and on this panel.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - IP stack - selection
Command ===> ____________________________________________________________

Jobname . . . . . . . . ________  (jobnname or filter)
Procname  . . . . . . . ________  (procnname or filter)
```

Figure 271. IP stack - selection - AUTOLOG

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function (F1). See "IPAUTOL - Communications Server IP autolog report" on page 496 for more information about the IP_AUTOLOG report.

IP stack resolver configuration data - Specifying selection criteria

When you select the **Resolver** option on the Resource - IP stack Selection panel (Figure 263 on page 384), an IP stack resolver configuration data report is generated. For more information about this report, see "IPRESOLV - Communications Server resolver report" on page 497.

Specifying output and run options

On the Resource - IP stack Selection panel (Figure 263 on page 384), you can use the Output/Run options to customize settings to run the report and generate output.

The output and run option settings you specify on the IP stack selection panels are saved in your ISPF profile and become the default settings for all IP stack panels that provide the option.

- To change the default setting on a panel, remove the selection from the field.
- To enable an option, enter an / in the input field for the option.
- If an option requires additional information and the information has not been specified, a panel opens so you can specify the information when you press Enter to run the query.
- If you select multiple options, the panels are presented in sequence until all required output and run parameters are specified.

Table 190 describes the available output and run options.

Table 190. Description of output and run options

Output/Run option	Description
Output in print format	Check this option to generate a printable report. When this option is selected, you can also use the options to customize the report title and send the report using email.
Customize title	Allows you to change the default report title. If you select this option, a panel is displayed so you can confirm or change the default report title. (See Figure 272 on page 390.) This option is only available when the **Output in print format** option is selected.

Table 190. Description of output and run options (continued)

Output/Run option	Description
Send as e-mail	If **Output in print format** is selected, you can select this option to send the report using e-mail. When you select this option, a panel opens where you can specify the e-mail information. Before configuring the e-mail information, you must configure the SMTP options with SETUP OUTPUT first. See "SE.7 Setup - Output" on page 1665.
Run in background	Determines whether the UNIX records processing is to proceed in the foreground or is to be submitted as a background (batch) job. This selection is only honored if Output in print format is also selected.

If you select the **Customize title** options, the panel shown in Figure 272 is displayed so you can specify the new titles.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Confirm or change page headers
Command ===> ____________________________________________________________________
Site title
> ________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

Report title
> All TCP/IP stack information ___________________________________________________
________________________________________________________________________________
________________________________________________________________________________
```

Figure 272. Page header Customization panel

UNIX filesystem reports (RE.U)

When you select option RE.U, the Resource - Unix panel shown in Figure 273 opens.

```
  Menu         Options       Info    Commands     Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Resource - Unix
Option  ===> ____________________________________________________________________


F    Filesystem      Unix filesystem selection
R    Reports         Unix audit reports
```

Figure 273. Resource Unix Menu

Filesystem - Unix filesystem reports

This option can be used to select and display Unix file system records. A full `CKFREEZE` data set read is required, and the `CKFREEZE` data set must have been made with the `UNIX=Y` parameter. If the zSecure Collect run was APF-authorized, additional information is displayed.

When you select option RE.U, the Resource - Unix Selection panel shown in Figure 274 on page 391 opens.

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> _____________________________________________________   _ start panel

Show Unix files that fit all of the following criteria:
File  . . _____________________________________________________________________
Complex . ________     (complex or EGN mask)

Advanced selection criteria
_  File attributes         _  File system             _  File ACL

Output/run options
_  Output in print format  _  Customize title         _  Send as e-mail
  _  Run in background
```

```
 Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> _____________________________________________________   _ start panel

Show Unix files that fit all of the following criteria:
File  . . _____________________________________________________________________
Complex . ________     (complex or ACF2 mask)

Advanced selection criteria
_  File attributes         _  File system             _  File ACL

Output/run options
_  Output in print format  _  Customize title         _  Send as e-mail
  _  Run in background
```

Figure 274. Resource Unix selection panel

If the selection panel is left blank, all UNIX records are selected. You can limit the UNIX records selected by completing one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For a description of the selection fields and to determine whether a field supports filters, use the field-sensitive help function.

Advanced selection criteria

On the Resource - Unix Selection panel (Figure 274), you can select one of the Advanced selection criteria to specify filters to select and display Unix filesystem records. When you select a criteria, a panel opens where you can specify the attributes in which you are interested. Information about each Advanced Selection criteria option is provided in the following sections.

File attributes: Selecting the check box on the Resource - Unix Selection panel (Figure 274) opens the panel shown in Figure 275 on page 392 where you can specify the file attributes you are interested in.

See the online help for detailed field descriptions.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> ____________________________________________________________________
All Unix files
Show unix files that fit all of the following criteria:
UID  . . . . . . . __________              (Decimal UID, no mask)
GID  . . . . . . . __________              (Decimal GID, no mask)
Owner  . . . . . . ________                (owner or EGN mask)
Group  . . . . . . ________                (group or EGN mask)
SECLABEL . . . . . ________                (SECLABEL or EGN mask)

File access (u/g/o/ug/uo/go/a/*)        File attributes (Y/N)
     Allowed      Disallowed              _  setuid        _  APF
 __  Read     __  Read                    _  setgid        _  Progam control
 __  Write    __  Write                   _  sticky bit    _  _BPX_SHAREAS
 __  Execute  __  Execute                                  _  Shared library

 Audit flags (-/s/f/a)                   File type
 _  Read         1. User                 /  Regular file   /  Pipe
 _  Write        2. Auditor              /  Directory      /  Socket
 _  Execute      3. Effective            /  Symbolic link  /  Character special
                                         /  External link  /  Block special
```

Figure 275. Resource Unix file attributes selection panel

File system: Selecting the **File system** check box on the Resource - Unix Selection panel (Figure 274 on page 391) opens the panel shown in Figure 276 where you can specify the file system names and attributes you are interested in.

See the online help for detailed field descriptions.

Figure 276. Resource Unix file system selection panel

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> ____________________________________________________________________
All Unix files
Show unix file systems that fit all of the following criteria:
Data set name  . . ____________________________________________
Mount point  . . . ____________________________________________________________
Owning system  . . ____                    (system or EGN mask)
Sysplex  . . . . . ________                (sysplex or EGN mask)
Volume serial  . . ______                  (volume or EGN mask)

Mount options (Y/N/Blank)
OR   _  SECURITY
     _  SETUID
     _  READ/WRITE
```

File ACL: Selecting the **File ACL** check box on the Resource - Unix Selection panel (Figure 274 on page 391) opens the panel shown in Figure 277 on page 393 where you can select on the presence of file access lists. The following panel is displayed when you check this option.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Resource - Unix Selection
Command ===> ____________________________________________________________________
All Unix files
Access list selection (Y/N/Blank)
OR   _  Directory has a file default access list
     _  Directory has a directory default access list
     _  File or directory has an extended access list
```

Figure 277. Resource Unix ACL selection panel

Output/Run options

On the Resource - Unix Selection panel (Figure 274 on page 391), you can use the Output/Run options to customize settings to run the report and generate output.

The output and run option settings you specify on the Unix selection panels are saved in your ISPF profile and become the default settings for all Unix panels that provide the option.

- To change the default setting on a panel, remove the selection from the field.
- To enable an option, enter an / in the input field for the option.
- If an option requires additional information and the information has not been specified, a panel opens so you can specify the information when you press Enter to run the query.
- If you select multiple options, the panels are presented in sequence until all required output and run parameters are specified.

Table 191 describes the available output and run options.

Table 191. Description of output and run options

Output/Run option	Description
Output in print format	Check this option to generate a printable report. When this option is selected, you can also use the options to customize the report title and send the report using e-mail.
Customize title	Allows you to change the default report title. If you select this option, a panel is displayed so you can confirm or change the default report title. This option is only available when the **Output in print format** option is selected.
Send as e-mail	If **Output in print format** is selected, you can select this option to send the report using e-mail. When you select this option, a panel opens where you can specify the e-mail information. Before configuring the e-mail information, you must configure the SMTP options with SETUP OUTPUT first. See “SE.7 Setup - Output” on page 1665.
Run in background	Determines whether the UNIX records processing is to proceed in the foreground or is to be submitted as a background (batch) job. This selection is only honored if Output in print format is also selected.

Unix records display

After processing the CKFREEZE file, the UNIX summary panel opens to display the results as shown in Figure 278.

```
IBM Security zSecure UNIX summary                          Line 1 of 26
Command ===> _____________________________________________ Scroll===> CSR_
All Unix files                                  28 Aug 2008 00:07
   Complex System  Count
   EEND     EEND     70562
   Count FS mount point
__    24  /
__     2  /home
__     2  /home/crmbhg1
__   205  /u
__     5  /u/automount
__  1713  /u/automount/c2eaudit
__  3105  /u/automount/c2rnew
__   446  /u/automount/smpe
__   730  /u/automount/smpe/smpnts/STP82890/SMPPTFIN
__  1434  /u/automount/C2RSRV#P
__   283  /u/automount/C2RSRV#P/PZ00350
__     1  /u/automount2
__     1  /u/zosmapper
__    11  /EEND
```

Figure 278. Unix summary display

The following table describes the fields of interest on the UNIX summary panel.

Table 192. UNIX summary panel - fields of interest

Field	Description
Complex	The complex name.
System	The system name.
Count	The total number of files in the file system.
FS mount point	The directory where the file system is mounted.

Viewing UNIX files for a selected mount point: Selecting any of the mount points listed in the UNIX summary panel (Figure 278) displays the list of UNIX files for that mount point as shown in Figure 279.

You can perform the following actions from the UNIX file list display panel:

- Enter **B** to browse the regular files.
- Enter **I** for a file or directory to call the UNIX System Services ISPF Shell
- For directories, enter the **U** action command to start the z/OS UNIX Directory List Utility

Figure 279. UNIX summary panel - Unix file list for selected mount point

```
IBM Security zSecure UNIX summary                          Line 1 of 446
 Command ===> ____________________________________________ Scroll===> CSR_
 All Unix files                                  28 Aug 2008 00:07
    Complex System  Count
    EEND     EEND     70562
    Count FS mount point
      446  /u/automount/smpe
    T FileMode +  apsl AuF Owner    Group    Relative pathname (within FS)
__ d rwx------        fff CRMBHJ1  ZSECUR   .
__ d rwx------        fff CRMBHJ1  LDAP     smpnts
__ l                  fff CRMBHJ1  LDAP     smpnts/zos19jpn
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XML
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/GIMPAF.XSL
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPHOLD/S0004.ESMCP
__ d rwx------        fff CRMBHJ1  ZSECUR   smpnts/STP82890/SMPPTFIN
__ d rwx------        fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
__ - rw-------   --s- fff CRMBHJ1  LDAP     smpnts/STP82890/SMPRELF/CPPCACHE.IB
```

The following table provides the field descriptions for the UNIX file list display.

Table 193. UNIX file list display - fields of interest

Field	Description
T	File type. This field can have any of the following values: **-** regular file **b** block special file **c** character special file **d** directory **e** external symlink **l** symlink **p** pipe **s** socket
Filemode	The effective file mode, shown as lists of permissions for specific groups. The groups can be any of the following: *o* owner *g* group *o* other An *a* indicates that the permissions of all groups are equal. The permissions can be any of the following: *r* read *w* write *e* execute *s* setup/setgid *S* setup/setgid when execute permission is off *t* sticky bit *T* sticky bit when execute permission is off Note that this format is the same as used by the `chmod` command.

Table 193. UNIX file list display - fields of interest (continued)

Field	Description
+	Indicates whether a file has any (extended) ACL entries; these can be any of the following types of entries: access directory default file default
apse	The effective extended attributes, shown as a list of attributes that are on (+) and a list of attributes that are off (-). Attributes can be any of the following: *a* authorization *p* program controlled *a* address space sharing *l* library sharing An *a* indicates that the permissions of all groups are equal. The permissions can be any of the following: *r* read *w* write *e* execute *s* setup/setgid *S* setup/setgid when execute permission is off *t* sticky bit *T* sticky bit when execute permission is off Note that this format is the same as used by the `chmod` command.
AuF	The combined audit flags: three positions for read, write, and execute access. Each position indicates the audit flag setting which can be any of the following: *s* successes *f* failures *a* all - none *Combined* either the owner or auditor has requested auditing
Owner	The RACF `userid` that is mapped to the owning UID. If there are several such RACF user IDs, this is the alphabetically first one.
Relative pathname (within FS)	Path name relative to the file system's mount point.

Viewing UNIX file details: When you browse a file from the UNIX file list display panel shown in Figure 279 on page 394, the UNIX file detail display panel shown in Figure 280 on page 397 opens. To browse the contents of a file in this panel, type **B** in front of the **Absolute pathname** field.

```
IBM Security zSecure UNIX summary                          Line 1 of 57
Command ===> _____________________________________ Scroll===> CSR_
All Unix files                                 28 Aug 2008 00:07




  System view of file
  Complex name                  EEND
  Sysplex name                  NLDLPPLX
  System name                   EEND
_ Absolute pathname             /u/automount/smpe/smpnts/STP82890/GIMPAF.XML
  FS mounted with SECURITY      Yes
  FS mounted with SETUID        No
  FS mounted READ/WRITE         Yes
  File access attributes        go=,u=rw
  Security label
  Extended file attributes      +s -apl
  Effective audit flags         =f
_ Owner name                    CRMBHJ1 CRMQA097 HZSUSER LDAPSRV OMVS RCCSL01
_ Owner name                    SKRBKDC STRCONS STRTASK TCPSRV
_ Group name                    LDAP SMPE
  Home Directory for Users
  Device                        1648
  Relative audit priority
  Audit concern

  Physical file attributes
  Complex that owns file system EEND
  System that owns file system  EEND
  File system data set name     CRMBOMVS.U.SMPE.HFS
  Volume serial for file system SMPNTS
  File system DASD serial + id  IBM-68-000000065892-0062
  Relative pathname within FS   smpnts/STP82890/GIMPAF.XML
  File type                     -
  Physical access attributes    o=,u=rw,g=r
  Physical extended attributes  +s -apl
  User-requested audit flags    =f
  Auditor-specified audit flags =
  User id                       0
  Group id                      3
  Inode number                  98
  File audit id                 01E2D4D7D5E3E2000F05000000620000
  Number of hard links          1

  User     TOrwx ACL id   UID/GID    Name                 InstData
  CRMBHJ1   urw- CRMBHJ1  0          JOHN FRANK
  CRMQA097  urw- CRMQA097 0          TEST QUOTED FORMAT   OMVS HOME TO TEST $QU
  HZSUSER   urw- HZSUSER  0                               Z/OS HEALTH CHECKER
  LDAPSRV   urw- LDAPSRV  0          LDAP SERVER USER
  OMVS      urw- OMVS     0
  RCCSL01   urw- RCCSL01  0          JOHN SMEDLINE SPEC.
  SKRBKDC   urw- SKRBKDC  0          KERBEROS STARTEDTASK NETW AUTH KERBEROS
  STRCONS   urw- STRCONS  0          STC VOOR TSO CONSOLE
  STRTASK   urw- STRTASK  0          DIV STARTED TASK USR
  TCPSRV    urw- TCPSRV   0          TCPIP STARTED TASK
  -group-   gr-- LDAP     3
  -group-   gr-- SMPE     3
  - any -   o--- -other-  n/a




****************************** Bottom of Data ******************************
```

Figure 280. Unix detail display

For details on the fields available on this display, see the following sections.

- "System view of file" on page 398
- "Physical file attributes" on page 399
- "UNIX access lists" on page 400

System view of file: This section shows the effective settings. For example, the absolute `pathname` consists of the relative `pathname` within the HFS or zFS data set, prefixed by the mount point of the file system. The effective flags take the mount attributes and mode into account.

Table 194 lists the fields available in this section.

Table 194. UNIX file detail display - System view of file fields

Field	Description
Complex name	The complex name.
Sysplex name	The sysplex name.
System name	The system name.
Absolute pathname	The full path name for the file. To view the contents of the file, type **B** in this field.
FS mounted with SECURITY	Whether the file system is mounted with the SECURITY attribute. If not, any user can access and change any file in it.
FS mounted with SETUID	Whether the file system is mounted with the SETUID attribute. Setuid, setgid, APF, and program control attributes are only honored when the file system is mounted.
FS mounted READ/WRITE	The mode in which the file system is mounted: READ The file system is mounted read-only; RDWR The file system is mounted read/write.
File access attributes	The effective file mode, shown as lists of permissions for specific groups. The group type is indicated by any of the following values. *o* for owner *g* for group *o* for other *a* for all The permissions can be *r* read *w* write *e* execute *s* setuid and setgid *t* sticky bit (setuid is shown with *u*, setgid with *g*).
Security label	The security label for the file.
Extended file attributes	The effective extended attributes, shown as a list of attributes that are on (+) and a list of attributes that are off (-).
Effective audit flags	The effective audit flags, shown as lists of the following values, or as a single list if the access type does not matter. *f* failures *s* successes for the access types *r* read, *w* write *x* execute
Owner name	The RACF `userid` that maps to the UID for the file. If there are more such users, a list is shown.
Group name	The RACF group that maps to the GID for the file. If there are more such groups, a list is shown.

Table 194. UNIX file detail display - System view of file fields (continued)

Field	Description
Home Directory	This repeated field can only be filled in for a directory. It lists the users for whom this directory is their home directory.
Device	The device number identifying the mount point.
Relative audit priority	The audit priority for this file.
Audit concern	The audit concerns identified for this file. See "UNIX: UNIX System Services File System" on page 1480 for a list of the audit concerns that can be identified.

Physical file attributes: This section shows the physical characteristics, such as the flags actually indicated in the file system itself.

Table 195. UNIX file detail display - Physical file attributes fields

Field	Description
Complex that owns file system	Complex of the system that owns the file system.
System that owns file system	System that owns the file system.
File system data set name	The name of the data set that holds the file system.
Volume serial for file system	The volume serial of the HFS or zFS data set.
File system DASD serial + id	Manufacturer/Factory/Serial identifying the DASD, and device tag id (port) assigned to this volume on the owning system.
Relative pathname within FS	Path name relative to the file system's mount point.
File type	The type of file. The UNIX file types are: *-* regular file *d* directory *p* pipe (or FIFO) *b* block special file *e* external symlink *s* socket *c* character special file *l* symlink.

Table 195. UNIX file detail display - Physical file attributes fields (continued)

Field	Description
Physical access attributes	The physical file mode shown as lists of permissions for specific groups. The group type is indicated by the following values: *o* for owner *g* for group *o* for other *a* for all The permissions can be *r* for read *w* for write *x* for execute *s* for set gid *u* for sticky bit setuid *g* for sticky bit setgid
Physical extended attributes	The physical extended attributes, shown as a list of attributes that are on (+) followed by a list of attributes that are off (-).
User-requested audit flags	The audit flags requested by the owner, shown as lists of the following values, or as a single list if the access type does not matter. *s* successes *f* failures *r* read *w* write *x* execute
Auditor-specified audit flags	The audit flags specified by the auditor, shown similarly.
User id	The UID for the file.
Group id	The GID for the file.
Inode number	The inode number for the file. This number identifies the file within the file system.
File audit id	The audit ID for the file.
Number of hard links	The number of directory entries for the file. Note that a UNIX file has no canonical path name; the inode identifies a file within the file system. File and other attributes are associated with the inode, not the path name.

UNIX access lists: Shows the UNIX access lists. An access ACL can be shown for any file type. For a directory, a directory default and a file default ACL can also be shown.

The UNIX access control list contains the following fields.

Table 196. UNIX file detail display - Access control list fields

Field	Description
User	The user to which the entry pertains. This field can show any of the following values: • *-group-* in an unexpanded ACL (or in an exploded ACL, for an empty group); in that case the **ACL id** field shows the group • *-undef-* in an unexpanded or exploded ACL for a UID or GID that does not correspond with a RACF user or group (as appropriate). • *-any-* shows the global access setting.
TOrwx	This field indicates the ACL type, origin, and user access permissions: ACL Type (**T**) can be any of the following: *d*directory default *f* file default blank access + ACL entry *a* auditor attribute *r*, *w*, *x* indicates the user access; read, write or execute ACL entry Origin (**O**) can be any of the following: *u* owning user *g* owning group *o* other User access permissions *r* read access *w* write access *x* execute access
ACL id	A RACF user or group associated with the UID/GID. This column can show a RACF user or group, or special origin values *-other-* for the global access setting (User *-any-*), *-owner-* for a file owner UID *-group-*for an owning group GID *-ACLuid-* for a UID on the ACL *-ACLgid-* for a GID on the ACL *-audit-* for directory read/execute access through the system-wide AUDITOR attribute *-more-* when an actual access level has more than one origin.

Table 196. UNIX file detail display - Access control list fields (continued)

Field	Description
UID/GID	The UID or GID that grants this access or an indication why none applies. If the column shows a number, this is a UID if **User** and **ACL id** are equal (if a RACF identity was determined), and also if **ACL id** contains *-owner-* or *-ACLuid-* (if not). Otherwise it is a GID. This column shows *n/a* for the global access setting (User *-any-*), for a composite entry (ACL id *-more-*), or when r-x access to a directory is granted to a user on the basis of the RACF auditor attribute. In an exploded ACL, this column can show *-no uid-* or *-no gid-* for RACF auditor user that has no access to UNIX because there is no associated GID or UID, either directly or through BPX.DEFAULT.USER.
Name	The user name.
InstData	The installation data for the user or group.

CICS resource reports

The **RE Resource reports** option on the zSecure Audit Main menu shown in Figure 262 on page 383 allows you to select and display CICS region, transaction, and program data. The report data is obtained from a CKFREEZE data set that is created by running zSecure Collect APF-authorized.

Select **RE.C** from the zSecure Audit Main menu to display the CICS Resource panel shown in Figure 281.

The **T** and **P** options are features provided by the zSecure Audit products.

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                    zSecure Suite - Resource - CICS
Option  ===> ____________________________________________________________

R   Regions       CICS region reports
T   Transactions  CICS CICS transactions selection and reports
P   Programs      CICS programs selection and reports
```

Figure 281. CICS Resource panel

CICS region reports

In the CICS Resource panel in Figure 281, select the **R** menu option to display the CICS Regions selection panel in Figure 282 on page 403.

Use this panel to enter selection criteria in one or more fields to limit the CICS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

You can also select output and run options in the CICS Regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS region records that

match your selection criteria.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                    zSecure Suite - CICS - Regions
Command  ===> ____________________________________________________________

Show CICS regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ________  (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings  _  Region attributes   _  Classes

Output/run options
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

Figure 282. CICS Regions selection panel

In Figure 282, you can select advanced selection criteria. When you select **Region security settings**, the following panel is displayed.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                zSecure Suite - CICS - Regions security settings
Command  ===> ____________________________________________________________

Show CICS regions that fit all of the following security criteria
Default userid  . . . . ________  (userid or filter)
Region userid . . . . . ________  (userid or filter)
PLT userid  . . . . . . ________  (userid or filter)
PLT security  . . . . . _  1. None  2. Cmdsec  3. Ressec   4. All
Security prefix . . . . _  1. Yes   2. No      3. Prefix or filter  _________
Keyring for SSL . . . . ____________________________________________________

Select region security settings (Y/N/blank)
OR   (AND or OR relationship)
_  ESM invoked                        _  Surrogate user checking
_  Always do CMD. checking            _  Journal security
_  Always do RES. checking            _  DB2 entry security
_  Attached transaction security      _  Started transaction security
_  Program security                   _  PSB security
_  Command security                   _  Generic resource security
_  File security                      _  Unix file security
_  Transient data security            _  APPCLU for sessions checking
_  Temp storage security              _  EJBROLE for EJB checking
```

Figure 283. CICS Regions security settings

In Figure 282, under advanced selection criteria, select **Region attributes** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                  zSecure Suite - CICS - Regions attributes
Command  ===> ____________________________________________________________

Show CICS regions that fit all of the following attribute criteria
VTAM Specific applid    ________  (applid or filter)
VTAM Generic applid . . ________  (applid or filter)
VTAM CICSPLEX applid    ________  (applid or filter)
CICS SVC Number . . . . ____________________  (comma separated list)
CICS HPO SVC Number . . ____________________  (comma separated list)

Select region attributes (Y/N/blank)
OR   (AND or OR relationship)
_  Storage protection                  _  Workarea storage in CICS Key
_  Transaction isolation               _  TCT User area in CICS key
_  Storage protection CICS cmd         _  TCT User area location above
_  Task storage checking               _  RENT program protection
_  Terminal storage checking           _  Use LLACOPY for modules
_  CICS High Performance option        _  Load modules from LPA
```

Figure 284. CICS Regions attributes

In Figure 282 on page 403, under advanced selection criteria, select **Classes** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                  zSecure Suite - CICS - Regions classes
Command  ===> ____________________________________________________________

Specify region classes selection criteria
Attached Transactions  . . . ________  (class or filter)
DB2 Entry  . . . . . . . . . ________  (class or filter)
Files  . . . . . . . . . . . ________  (class or filter)
General Resources  . . . . . ________  (class or filter)
Journals . . . . . . . . . . ________  (class or filter)
Programs . . . . . . . . . . ________  (class or filter)
Program Specification Blocks ________  (class or filter)
Started Transactions . . . . ________  (class or filter)
System Programming commands  ________  (class or filter)
Temporary Storage  . . . . . ________  (class or filter)
Transient Data . . . . . . . ________  (class or filter)
```

Figure 285. CICS Regions classes

In Figure 286 on page 405, the CICS region display report lists the CICS region configuration settings.

The data for the region display report is available only if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

Detailed field information is available by pressing F1 on the CICS regions display panels or on any field in the display panels. Descriptions of CICS region field names are also provided in “CICS_REGION: CICS regions” on page 974.

A sample overview display panel for the CICS regions display report is shown in Figure 286 on page 405.

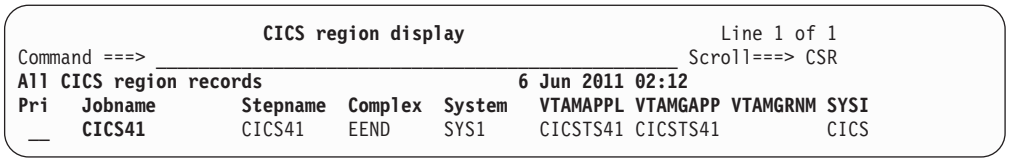


Figure 286. CICS region overview display report

A sample detail display panel for the CICS regions display report is shown in Figure 287 on page 406.

```
                    CICS region display                      Line 1 of 69
Command ===> ____________________________________________ Scroll===> CSR
All CICS region records                    6 Jun 2011 02:12

Region identification
  Complex name                    EEND
_ System name                     SYS1
  CICS Region job name            CICS41  Jobid STC03306 ASID 003A
  CICS Region step name           CICS41
  VTAM Specific applid            CICSTS41
  VTAM Generic applid             CICSTS41
  VTAM CICSPLEX Generic applid
  CICS System identification      CICS
  CICS System release level       TS 4.1.0
_ Default Userid                  CICSUSER     CICSA default user  Dfltgrp: SYS1
_ Region Userid                   CICSA        STC default user    Dfltgrp: STCGRP
_ PLT initialization userid       CICSPLT                          Dfltgrp: SYS1

SAF protection settings        SIT   Class      Act   Gen
Command security                Yes  CCICSCMD   Yes   No
DB2 Entry security              No
Transient Data security         No
File security                   No
Journal security                Yes   JCICSJCT   Yes   No
Started Transaction security    Yes   ACICSPCT   Yes   No
Program security                Yes   MCICSPPT   Yes   No
PSB security                    Yes   PCICSPSB   Yes   No
Generic Resource security       Yes   RCICSRES   Yes   No
Attached Transaction security   Yes   TCICSTRN   Yes   No
Temp. Storage security          Yes   SCICSTST   Yes   No
Sessions checked in APPCLU      No
EJBeans checked in EJBROLE      Yes   EJBROLE    Yes   No
Users checked in SURROGAT       Yes   SURROGAT   Yes   Yes

SAF protection extent                    CICS SVC numbers
ESM invoked                     Yes      Supervisor Call (SVC) Number  216
Always do CMD checking          No       HPO SVC Number
Always do RES checking          No
PSB check remote users          No
PLT initialization security     ALL
Resource Prefix                 CICSA.
EJBROLE Prefix
Keyring for SSL and Web
SSL Encryption strength         Strong

Region attributes
CICS Storage protection          Yes      Common workarea in CICS-key     No
Transaction isolation            Yes      TCT User area in CICS-key       No
Storage protection CICS cmd      Yes      TCT User area location above    No
Task storage checking            No       RENT program protection         No
Terminal storage checking        No       Load modules from LPA           No
High Performance Option (HPO)    No       Use LLACOPY for modules         No
Show user data in VTAM trace     No       Show user data in CICS trace    No
Autoinstall exit                 DFHZATDX Autoinstall console             N
Res.Def.Grps loaded at start     XYZLIST

CICS DFHCSD data set name                Disp  R/O
DFH410.CICS.DFHCSD                       Old   No

Good morning/night settings
Good morning transaction    CSGM
Good night transaction
Good morning text           This is the CICS41 system.

Private module list
DFHSIP
IEFBR14

Pri Audit concern
```

Figure 287. CICS region detailed display report

CICS transaction reports

In the CICS Resource panel in Figure 281 on page 402, select the **T** menu option to display the CICS Transactions selection panel in Figure 288.

Use this panel to enter selection criteria in one or more fields to limit the CICS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options in the CICS Transactions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS transaction records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                zSecure Suite - CICS - Transactions
Command  ===> ____________________________________________________________

Show CICS transactions that fit all of the following criteria:
Transaction . . . . . ____      (transaction or filter)
Program . . . . . ________  (program name or filter)
Jobname . . . . . ________  (jobname or filter)
VTAM applid . . . . . ________  (applid or filter)
SYSIDNT . . . . . ____      (identifier or filter)
Complex . . . . . ________  (complex or filter)
System  . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings    _  Attributes

Output/run options
1  0. No summary        1. Summarize by region  2. Summarize by transaction
_  Print format            Customize title         Send as e-mail
      Background run       Full page form
```

Figure 288. CICS Transactions selection panel

In Figure 288, you can select advanced selection criteria. When you select **Security settings**, the CICS Transactions security attributes panel in Figure 289 on page 408 is displayed.

In Figure 289 on page 408, the **RACF profile class** and **RACF profile name** fields select resources by using the merged in-storage profile built during the RACLIST process. If either the specified RACF profile class or the specified RACF profile name contributed to the in-storage profile, the resource is included in the report. The specified RACF profile name does not need to be defined in the specified RACF profile class for the resource to be included in the report.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - CICS - Transactions security attributes
Command  ===> ____________________________________________________________________

Show CICS transactions that fit all of the following access criteria
RACF profile class  . . ________       (class or filter)
RACF profile name . . . _____________  (profile or filter)
RACF Universal access   __  6  1. None     3. Update   5. Alter
                               2. Read     4. Control  6. Ignore
                               (operator: < <= > >= = <> ¬= )
```

Figure 289. CICS Transactions security attributes

In Figure 288 on page 407, under advanced selection criteria, select **Attributes** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - CICS - Transactions attributes
Command  ===> ____________________________________________________________________

Show CICS transactions that fit all of the following attribute criteria
Transaction class . . . ________  (class or filter)
Transaction priority    __  ___   (operator + 0-255)
Transaction alias . . . ____      (alias or filter)
Remote transaction name ____      (name or filter)
Remote system name  . . ____      (system or filter)
Transaction APPC name   ________________________________________________

Select transaction attributes (Y/N/blank)
OR   (AND or OR relationship)
_  Resource security checking          _  Command security checking
_  Enabled                             _  Enabled during shutdown
_  Task data location above            _  Dynamic routable
_  Task data in user key               _  Routable transaction
_  Task storage clearance              _  Use local queueing
_  Task storage freeze                 _  Dump if abnormal end
_  Transaction isolation               _  Restart after abnormal end
_  System purgeable                    _  Terminal-error purgeable
_  Trace transaction                   _  Trace confidential data
```

Figure 290. CICS Transactions attributes

In Figure 291 on page 409, the CICS transactions display report lists the CICS transaction settings.

The data for this report is only available if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

Detailed field information is available by pressing F1 on the CICS transaction display panels or on any field in the display panels. Descriptions of CICS transaction field names are also available in “CICS_REGION: CICS regions” on page 974.

```
                    CICS transaction display                    Line 186 of 190
Command ===> ____________________________________________________ Scroll===> CSR
All CICS transaction records                    6 Jun 2011 02:12
   Pri Tran Jobname  Stepname Complex       VTAMAPPL SYSIDNT  Program  Res Cmd
__     HPJC CICS41   CICS41   EEND          CICSTS41 CICS     DFHMIRS
__     QWAS CICS41   CICS41   EEND          CICSTS41 CICS     DFHEDAP
__     RTCK CICS41   CICS41   EEND          CICSTS41 CICS     CQTPCHEK
__     RTMM CICS41   CICS41   EEND          CICSTS41 CICS     CQTP0000
__     RTST CICS41   CICS41   EEND          CICSTS41 CICS     CQTPSTRT
```

Figure 291. CICS transaction overview display report

A sample detail display panel for the CICS transaction display report is shown in Figure 292 on page 410.

The **Class** and **Profile** fields show the grouping and member class profiles that contributed to the merged in-storage profile for the resource as established during the RACLIST process. The access list that follows shows the access to this merged in-storage only profile. The display format of the access list can be managed using the ACL primary command.

```
 CICS transaction display                              Line 1 of 53
Command ===> _____________________________________________ Scroll===> CSR
All CICS transaction records                    6 Jun 2011 02:12

Transaction identification
  Complex name                      EEND
_ System name                       SYS1
  Transaction name                  CEDA
  Resource name                     CICSA.CEDA
  First program name                DFHEDAP
  CICS Region job name              CICS41   Jobid STC03306 ASID 003A
  CICS Region step name             CICS41
  VTAM Specific applid              CICSTS41
  CICS System identification        CICS

Transaction security settings
Resource security checking       No     Command security checking       No

Transaction attributes
Enabled                          Yes    Enabled during shutdown          No
Task data location above         No     Use local queueing               No
Task data in user key            Yes    TWA size                         0
Task storage clearance           No     Task storage freeze              No
Trace transaction                Yes    Show user data in CICS trace     No
Transaction isolation            Yes    Transaction profile              DFHCICST
Transaction class                       Transaction Priority             1
Transaction alias                       Transaction Hex alias
Transaction PF/PA-key
Transaction APPC name

Transaction recovery attributes             Transaction remote attributes
System purgeable                Yes         Remote transaction name
Terminal-error purgeable        Yes         Remote system name
OTS Timeout                     0           Remote transaction profile
Indoubt wait action             Yes         Dynamic routable            No
Indoubt wait time               00:00       Routable transaction        No
Indoubt backout                 Yes
Dump if abnormal end            Yes
Restart after abnormal end      No
Deadlock timeout                0000
Runaway time                   00:00
Runaway time system             No

UACC
RACF Universal access      NONE

Class    Profile
GCICSTRN CICSA.SPRO

User       Access  ACL id   When
_ -group-  READ    SYSPROG
_ -group-  READ    SYSAUDIT
_ IBMUSER  READ    IBMUS

Pri Audit concern
```

Figure 292. CICS transaction detailed display report

CICS program reports

In the CICS Resource panel in Figure 281 on page 402, select the **P** menu option to display the CICS Programs selection panel in Figure 293 on page 411.

Use this panel to enter selection criteria in one or more fields to limit CICS program data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options in the CICS Programs selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the CICS program records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
             zSecure Suite - CICS - Programs
Command  ===> ____________________________________________________________

Show CICS programs that fit all of the following criteria:
Program . . . . . . . . ________  (program name or filter)
Program type  . . . . . 4  1. Program  2. Mapset  3. Partitionset  4. All
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
SYSIDNT . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings    _  Attributes

Output/run options
_  0. No summary        1. Summarize by region  2. Summarize by program
_  Print format            Customize title         Send as e-mail
         Background run    Full page form
```

Figure 293. CICS Programs selection panel

In Figure 293, you can select advanced selection criteria. When you select **Security settings**, the CICS Program security attributes panel in Figure 294 is displayed.

In Figure 294, the **RACF profile class** and **RACF profile name** fields select resources by using the merged in-storage profile built during the RACLIST process. If either the specified RACF profile class or the specified RACF profile name contributed to the in-storage profile, the resource is included in the report. The specified RACF profile name does not need to be defined in the specified RACF profile class for the resource to be included in the report.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - CICS - Program security attributes
Command  ===> ____________________________________________________________

Show CICS programs that fit all of the following access criteria
RACF profile class  . . ________       (class or filter)
RACF profile name . . . _____________  (profile or filter)
RACF Universal access   __  6  1. None     3. Update   5. Alter
                               2. Read     4. Control  6. Ignore
                               (operator: < <= > >= = <> ¬= )
```

Figure 294. CICS Program security attributes

Figure 293, under advanced selection criteria, select **Attributes** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - CICS - Programs attributes
Command  ===> ____________________________________________________________________

Specify remote selection criteria
Remote program name . . ________  (name of filter)
Remote transaction name ____      (name or filter)
Remote system name  . . ________  (system or filter)

Specify Java selection criteria
JVM Profile . . . . . . ____  (profile or filter)
Java main program class ____________________________________________________

Select program attributes (Y/N/blank)
OR   (AND or OR relationship)
_  Enabled                              _  Dynamic routable
_  Obtain new program copy              _  Allow CEDF (CICS Exec.Diag.Fac.)
_  Permanently load program             _  Use DPL-subset API
_  Task data location above             _  Task data in user key
_  Run in Java virtual machine
```

Figure 295. CICS Programs attributes

In Figure 296, the CICS program display report lists the CICS program settings.

The data for this report is available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating this file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

Detailed field information is available by pressing F1 on the CICS program display panels or on any field in the display panels. Descriptions of CICS program field names are also available in “CICS_PROGRAM: CICS programs” on page 970.

A sample overview display panel for the CICS program display report is shown in Figure 296.

```
                CICS program display                        Line 1780 of 1784
Command ===> ____________________________________________________ Scroll===> CSR
All CICS program records                        6 Jun 2011 02:12
Pri  Program  Type     Jobname  Stepname Complex   VTAMAPPL SYSIDNT  Ena
__   IXMI38DA Program  CICS41   CICS41   EEND      CICSTS41 CICS     Ena
__   IXMI38D1 Program  CICS41   CICS41   EEND      CICSTS41 CICS     Ena
__   IXMI38IN Program  CICS41   CICS41   EEND      CICSTS41 CICS     Ena
__   IXMI38UC Program  CICS41   CICS41   EEND      CICSTS41 CICS     Ena
__   IXM4C57  Program  CICS41   CICS41   EEND      CICSTS41 CICS     Ena
```

Figure 296. CICS program overview display report

A sample detail display panel for the CICS program display report is shown in Figure 297 on page 413.

The **Class** and **Profile** fields show the grouping and member class profiles that contributed to the merged in-storage profile for the resource as established during the RACLIST process. The access list that follows shows the access to this merged in-storage only profile. The display format of the access list can be managed using the ACL primary command.

```
  CICS program display                                Line 1 of 42
Command ===> ____________________________________________ Scroll===> CSR
All CICS transaction records                    6 Jun 2011 02:12

Program identification
  Complex name                    EEND
_ System name                     SYS1
  Program name                    CEEADJL
  Resource name                   CICSA.CEEADJL
  Program type                    Program
  CICS Region job name            CICS41    Jobid STC03306 ASID 003A
  CICS Region step name           CICS41
  VTAM Specific applid            CICSTS41
  CICS System identification      CICS

Program attributes
Enabled                          Yes        Dynamic routable              No
Obtain new program copy          No         Allow CICS Exec.Diag.Fac.     Yes
Permanently loaded program       No         Use DPL-subset API            No
Task data location above         Yes        Task data in user key         No
Use CICS API only (defined)      Yes        Use CICS API only (deduced)   Yes
Programming language(defined)    Undefined  Programming language(deduced)

Programs threadsafe(defined)  No            Programs threadsafe(deduced)  No

Remote program attributes
Remote program name                      Remote transaction name
Remote system name

Java settings
JVM Profile                   DFHJVMPR   Run in Java virtual machine   No
Java main program class

UACC
RACF Universal access         NONE

Class    Profile
PROGRAM CEE*

   User    Access   ACL id  When
_ -group-  READ     SYSPROG
_ -group-  READ     SYSAUDIT
_ IBMUSER  READ     IBMUSER

Pri Audit concern
```

Figure 297. CICS program detailed display report

IMS resource reports

The **RE Resource reports** option on the zSecure Audit Main menu shown in Figure 262 on page 383 allow you to select and display IMS region, transaction, and PSB data. The report data is obtained from a CKFREEZE data set created by running zSecure Collect APF-authorized.

Select **RE.M** from the zSecure Audit Main menu to display the IMS Resource panel shown in Figure 298 on page 414.

The **T** and **P** options are features provided by the zSecure Audit products.

```
Menu         Options       Info    Commands     Setup      Startpanel
-------------------------------------------------------------------------------
                          zSecure Suite - Resource - IMS
Option  ===> ____________________________________________________________

R   Regions         IMS control region reports
T   Transactions    IMS transactions reports
P   PSBs            IMS program specification blocks
```

Figure 298. IMS Resource panel

IMS region reports

In the IMS Resource panel in Figure 298, select the **R** menu option to display the IMS Regions selection panel in Figure 299.

Use this panel to enter selection criteria in one or more fields to limit the IMS region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

You can also select output and run options in the IMS Regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the IMS region records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                          zSecure Suite - IMS - Regions
Command ===> ____________________________________________________________

Show IMS control regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . ________    (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                Customize title        Send as e-mail
      Background run           Full page form
```

Figure 299. IMS Regions selection panel

In Figure 299, under advanced selection criteria, you can select **Region security settings** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                  zSecure Suite - IMS - Regions security settings
Command  ===> ____________________________________________________________________

Show IMS control regions that fit all of the following security criteria
Region userid  . . . . . ________  (userid or filter)
Resource class suffix    ________  (suffix or filter)
Security violation limit _         (0,1,2,or 3)
Console command option   _  1. Allow  2. Deny  3. RACF  4. Exit  5. RACF+Exit
Auto Oper CMD auth . . . _  1. Allow  2. SMU   3. RACF  4. Exit  5. RACF+Exit
Auto Oper ICMD auth  . . _  1. Allow  2. Deny  3. RACF  4. Exit  5. RACF+Exit
Select effective setting flags (Y/N/blank)
OR   (AND or OR relationship)
_  Perform user verification            _  User verification active
_  Perform transaction authorization    _  Transaction authorization active
_  ETO command authorization            _  Static/ETO command authorization
_  RACF resource access check           _  EXIT resource access check
_  RACF trans authorization available   _  TCO RACF security
_  Enable multiple sessions             _  Uppercase passwords only
Select requested region security settings by origin
_  System definition      _  JCL PARM override      _  /NRESTART override
```

Figure 300. IMS Regions security settings

In Figure 300, under region security settings by origin, select **System definition** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                  zSecure Suite - IMS - Regions sysdef
Command ===> ____________________________________________________________________

Select system definition flags (Y/N/blank)
OR   (AND or OR relationship)
_  User verify                          _  Force user verify
_  Transaction authorization            _  Force transaction authorization
_  ETO command authorization            _  Static/ETO command authorization
_  Enhanced security                    _  Call RACF
_  Enable multiple sessions
```

Figure 301. IMS Regions sysdef

In Figure 300, under region security settings by origin, select **JCL PARM override** to display the following panel.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                  zSecure Suite - IMS - Regions JCL parms
Command  ===> ____________________________________________________________________

Select JCL PARM override flags (Y/N/blank)
OR   (AND or OR relationship)
_  User verify                        _  Force user verify
_  ETO command authorization          _  Static/ETO command authorization
_  Enable multiple sessions           _  Uppercase passwords only
```

Figure 302. IMS Regions JCL parms

In Figure 300, under region security settings by origin, select **/NRESTART override** to display the following panel.

```
Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                 zSecure Suite - IMS - Regions /NRESTART
Command  ===> ____________________________________________________________

Select /NRESTART security flags (Y/N/M/blank)
OR   (AND or OR relationship)
_  User verify                          _  Transaction authorization
_  ETO command authorization            _  Static/ETO command authorization
_  Enable multiple sessions

   Y/N   : explicitly specified by operator
   M     : not specified by operator
   blank : don't use for selection
```

Figure 303. IMS Regions JCL parms

In Figure 296 on page 412, the IMS regions display report lists the IMS region configuration settings.

The data for this report is available only if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

Detailed field information is available by pressing F1 on the IMS region display panels or on any field in the display panels. Descriptions of the IMS region field names are also available in "IMS_REGION: IMS subsystems" on page 1042.

A sample overview display panel for the IMS region display report is shown in Figure 303.

```
                IMS region display                          Line 1 of 1
Command ===> ____________________________________________ Scroll===> CSR
All IMS region records                        6 Jun 2011 02:12
   Pri Jobname  Stepname Complex       System   VTAMAPPL RegType  IMSID    IMS
__     IMS10CR1 IMS10CR1 EEND          SYS1     IMS10CR1 Online   IVP1     V10M
```

Figure 304. IMS region overview display report

A sample detail display panel for the IMS region display report is shown in Figure 304 on page 416.

```
                IMS region display                              Line 1 of 51
Command ===> ____________________________________________ Scroll===> CSR
All IMS region records                        6 Jun 2011 02:12

Region identification
  Complex name                  EEND
_ System name                   SYS1
  IMS Region job name           IMS10CR1   Jobid STC03308 ASID 003C
  IMS Region step name          IMS10CR1
  VTAM Applid                   IMS10CR1
  IMS Region type               Online
  IMS System identification     IVP1
  IMS System release level      V10M10
  Console command character     /        IMS SVC number      203
_ Region userid                 START2               Dfltgrp: SYS1

Region security settings
Perform user verification       Yes    User verification active      Yes
Perform trans authorization     Yes    Trans authorization active    Yes
ETO cmd authorization           Yes    Stat/ETO cmd authorization    Yes
RACF resource access check      Yes    EXIT resource access check    No
Auto Oper ICMD auth.            Deny   Auto Oper CMD auth            RACF
RACF trans auth avail           Yes    TCO RACF security            No
Resource class suffix           IMS    Console command option        RACF
Uppercase passwords only        No     Security violation limit      2
Enable multiple sessions        Yes    Secure ODBA APSB requests     No

SAF protection settings       Class    Act  Gen
Command class                 CIMS     Yes  Yes
Field protection class        FIMS     Yes  Yes
Transaction class             TIMS     Yes  Yes
PSB class                     IIMS     Yes  No
LTERM class                   LIMS     Yes  No
Database class                PIMS     Yes  Yes
Other protection class        OIMS     Yes  Yes
Open trans mngr access class  RIMS     No   No
Segment protection class      SIMS     Yes  Yes

System definition flags
User verify                   Yes      Force user verify             Yes
Transaction authorization     No       Force trans authorization     Yes
ETO command authorization     No       Static ETO cmd authorization  No
Enhanced security             Yes      Call RACF                     Yes
Enable multiple sessions      Yes

JCL PARM override flags                /NRESTART security flags
User verify                   No       User verify                   No
Force user verify             No       Transaction authorization     No
ETO command authorization     Yes      ETO command authorization     No
Static ETO cmd authorization  Yes      Static ETO cmd authorization  No
 Enable multiple sessions     Yes      Enable multiple sessions      No
Uppercase passwords only      No

Pri Audit concern
```

Figure 305. IMS region detailed display report

IMS transaction reports

In the IMS Resource panel in Figure 298 on page 414, select the **T** menu option to display the IMS Transaction selection panel in Figure 305.

Use this panel to enter selection criteria in one or more fields to limit IMS transaction data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS transaction selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS transaction records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - Transactions
Command ===> ____________________________________________________________________

Show IMS transactions that fit all of the following criteria:
Transaction . . . . . . ________  (transaction or filter)
Transaction class . . . ____      (class number or filter)
Program specif. block   ________  (PSB or filter)
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced transaction selection criteria
_  Security settings
Output/run options
0  0. No summary        1. Summarize by region  2. Summarize by transaction
     _  Print format      Customize title         Send as e-mail
          Background run    /  Full page form
```

Figure 306. IMS Transactions selection panel

In Figure 306, you can select advanced selection criteria. When you select **Security settings**, the IMS Transactions security attributes panel in Figure 307 is displayed.

In Figure 307, the **RACF profile class** and **RACF profile name** fields select resources by using the merged in-storage profile built during the RACLIST process. If either the specified RACF profile class or the specified RACF profile name contributed to the in-storage profile, the resource is included in the report. The specified RACF profile name does not need to be defined in the specified RACF profile class for the resource to be included in the report.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - IMS - Transactions security attributes
Command  ===> ___________________________________________________________________

Show IMS transactions that fit all of the following access criteria
RACF profile class  . . ________       (class or filter)
RACF profile name . . . ____________   (profile or filter)
RACF Universal access   __  6  1. None     3. Update   5. Alter
                               2. Read     4. Control  6. Ignore
                               (operator: < <= > >= = <> ¬= )
```

Figure 307. IMS Transactions security attributes

In Figure 308 on page 419, the IMS transaction display report lists the IMS transaction settings.

The data for this report is available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

Detailed field information is available by pressing F1 on the IMS transaction display panels or on any field in the display panels. Descriptions of IMS transaction field names are also provided in “IMS_TRANSACTION: IMS transactions” on page 1048.

A sample overview display panel for the IMS transaction display report is shown in 419.

```
                IMS transaction display                          Line 21 of 25
Command ===> ____________________________________________________ Scroll===> CSR
 All IMS transaction records                    6 Jun 2011 02:12
    Pri     Trans    TRCl PSBName  Jobname  Stepname Complex       VTAMAPPL IMSID
__           IVTFD       1 DFSIVP4  IMS10CR1 IMS10CR1 EEND          IMS10CR1 IVP1
__           IVTFM       1 DFSIVP5  IMS10CR1 IMS10CR1 EEND          IMS10CR1 IVP1
__           IVTNO       1 DFSIVP1  IMS10CR1 IMS10CR1 EEND          IMS10CR1 IVP1
__           IVTNV       1 DFSIVP2  IMS10CR1 IMS10CR1 EEND          IMS10CR1 IVP1
__           PART        1 DFSSAM02 IMS10CR1 IMS10CR1 EEND          IMS10CR1 IVP1
```

Figure 308. IMS transaction overview display report

A sample detail display panel for the IMS transaction display report is shown in Figure 309 on page 419.

The **Class** and **Profile** fields show the grouping and member class profiles that contributed to the merged in-storage profile for the resource as established during the RACLIST process. The access list that follows shows the access to this merged in-storage only profile. The display format of the access list can be managed using the ACL primary command.

```
                  IMS transaction display                        Line 1 of 69
Command ===> ____________________________________________________ Scroll===> CSR
All IMS transaction records                   6 Jun 2011 02:12

Transaction identification
  Complex name                      EEND
_ System name                       SYS1
  Transaction                       ADDINV
  Resource name                     ADDINV
  Transaction class                 1
  Program specification block       DFSSAM04
  IMS Region job name               IMS10CR1 Jobid STC03308 ASID 003C
  IMS Region step name              IMS10CR1
  VTAM Applid                       IMS10CR1
  IMS System identification         IVP1

UACC
RACF Universal access         NONE

Class    Profile
GIMS     IVPGRP1
TIMS     ADDINV

User        Access  ACL id   When
_ B8FU0001  READ    B8FU0001
```

Figure 309. IMS transaction detailed display report

IMS PSB reports

In the IMS Resource panel in Figure 298 on page 414, select the **P** menu option to display the IMS PSBs selection panel in Figure 310.

Use this panel to enter selection criteria in one or more fields to limit IMS program specification block data. When you specify selection criteria, only those records that match all criteria are included in the output. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

To create a simulate report, use the report type option **Simulate access for specified resource**.

You can also select output and run options on the IMS PSBs selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of IMS PSB records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
              zSecure Suite - IMS - PSBs
Command ===> ____________________________________________________________________

Show IMS PSBs that fit all of the following criteria:
Program specif. block   ________  (PSB or filter)
Jobname . . . . . . . . ________  (jobname or filter)
VTAM applid . . . . . . ________  (applid or filter)
IMSID . . . . . . . . . ____      (identifier or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)
Type of report  . . . . 1  1. Show resource definitions
                           2. Simulate access for specified resource

Advanced PSB selection criteria
_  Security settings

Output/run options
0  0. No summary        1. Summarize by region  2. Summarize by transaction
     _  Print format       Customize title         Send as e-mail
          Background run    /  Full page form
```

Figure 310. IMS PSB selection panel

In Figure 310, you can select advanced selection criteria. When you select **Security settings**, the IMS Transactions security attributes panel in Figure 311 on page 421 is displayed.

In Figure 311 on page 421, the **RACF profile class** and **RACF profile name** fields select resources by using the merged in-storage profile built during the RACLIST process. If either the specified RACF profile class or the specified RACF profile name contributed to the in-storage profile, the resource is included in the report. The specified RACF profile name does not need to be defined in the specified RACF profile class for the resource to be included in the report.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
      zSecure Suite - IMS - security attributes
Command  ===> ____________________________________________________________________

Show IMS PSBs that fit all of the following security criteria
RACF profile class  . . ________       (class or filter)
RACF profile name . . . _____________  (profile or filter)
RACF Universal access   __  6  1. None     3. Update   5. Alter
                               2. Read     4. Control  6. Ignore
                               (operator: < <= > >= = <> ¬= )
```

Figure 311. IMS PSB security attributes

In Figure 312, the IMS PSBs display report lists the IMS PSB settings.

The data for this report is available only if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

Detailed field information is available by pressing F1 on the IMS PSB display panels or on any field in the display panels. Descriptions of IMS PSB field names are also available in "IMS_PSB: IMS program specification blocks" on page 1039.

A sample overview display panel for the IMS PSBs is shown in Figure 312.

```
                IMS PSB display                                  Line 44 of 47
Command ===> ____________________________________________________ Scroll===> CSR
All IMS PSB records                              6 Jun 2011 02:12
   Pri PSBName  Transact Jobname  Stepname Complex       VTAMAPPL IMSID    UACC
__      DFSSAM08          IMS10CR1 IMS10CR1 EEND        IMS10CR1 IVP1     READ
__      DFSSAM09          IMS10CR1 IMS10CR1 EEND        IMS10CR1 IVP1     READ
__      IPOPSB   IPOQRY   IMS10CR1 IMS10CR1 EEND        IMS10CR1 IVP1
__      IVPREXX  IVPREXX  IMS10CR1 IMS10CR1 EEND        IMS10CR1 IVP1
__
```

Figure 312. IMS PSB overview display panel

A sample detail display panel for the IMS PSB display report is shown in Figure 313 on page 422.

The **Class** and **Profile** fields show the grouping and member class profiles that contributed to the merged in-storage profile for the resource as established during the RACLIST process. The access list that follows shows the access to this merged in-storage only profile. The display format of the access list can be managed using the ACL primary command.

```
                    IMS PSB display                              Line 1 of 29
Command ===> ____________________________________________________ Scroll===> CSR
All IMS PSB records                              6 Jun 2011 02:12

PSB identification
  Complex name                  EEND
_ System name                   SYS1
  Program specification block   DFSIVP6
  Resource name                 DFSIVP6
  Transactions
  IMS Region job name           IMS10CR1   Jobid STC03308 ASID 003C
  IMS Region step name          IMS10CR1
  VTAM Applid                   IMS10CR1
  IMS System identification     IVP1

UACC
RACF Universal access         NONE
Class    Profile
JIMS     IVPGRP4
JIMS     IVPGRP3
JIMS     IVPGRP2
JIMS     IVPGRP1
IIMS     DFSIVP6

User        Access  ACL id   When
_ B8FU0001  READ    B8FU0001
_ B8FU0002  READ    B8FU0002
_ B8FU0003  READ    B8FU0003
_ B8FU0004  READ    B8FU0004

Pri Audit concern
```

Figure 313. IMS PSB detailed display report

DB2 resource reports

The **RE Resource reports** option on the zSecure Audit Main menu shown in Figure 262 on page 383 allow you to select and display DB2 region data.

Select **RE.D** from the zSecure Audit Main menu to display the DB2 regions selection panel shown in Figure 314 on page 423.

DB2 region reports

Use this panel to enter selection criteria in one or more fields to limit the DB2 region configuration data. When you specify selection criteria, the output includes only those records that match all the selection criteria. Filters can be used in some of the selection fields. To find out if a field supports filters, use the field-sensitive help function (F1).

You can also select output and run options in the DB2 regions selection panel, or select no options and report data is processed as soon as you press Enter. The overview panel that is displayed shows a summary of the DB2 region records that match your selection criteria.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - DB2
Command ===> ____________________________________________________________________

Show DB2 regions that fit all of the following criteria:
Jobname . . . . . . . . ________  (jobname or filter)
Local LU name . . . . . ________          (luname or filter)
Local site name . . . . ________________  (name or filter)
DB2ID . . . . . . . . . ____              (identifier or filter)
Group attachment name   ____              (name or filter)
Complex . . . . . . . . ________  (complex or filter)
System  . . . . . . . . ____      (system or filter)

Advanced selection criteria
_  Region security settings

Output/run options
_  Print format                Customize title       Send as e-mail
      Background run           Full page form
```

Figure 314. DB2 Region selection panel

In Figure 314, you can select advanced selection criteria. When you select **Region security settings**, the following panel is displayed.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
            zSecure Suite - DB2 - regions security settings
Command  ===> ____________________________________________________________________

Specify region security criteria
Region userid . . . . . . . ________  (userid or filter)
Classification option . . . _  1. Single-subsystem    2. Multi-subsystem
Class name root . . . . . . ____      (root or filter)
Class name suffix . . . . . _         (0-9, #, @, or $)

Classes used by DB2 (filters allowed)
Buffer pool privileges  . . ________  System privileges . . . . . ________
Collection privileges . . . ________  Stored procedure privileges ________
Database privileges . . . . ________  Sequences . . . . . . . . . ________
Java archive files  . . . . ________  Table,index,view privileges ________
Package privileges  . . . . ________  Tablespace privileges . . . ________
Plan privileges . . . . . . ________  User function privileges    ________
Schema privileges . . . . . ________  User type privileges  . . . ________
Storage group privileges    ________
```

Figure 315. DB2 region security settings

In Figure 315, the DB2 region display report lists the DB2 region configuration settings.

The data for this report is available only if a CKFREEZE file is created during an APF-authorized run of zSecure Collect (the CKFCOLL program). For details about creating a CKFREEZE file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

Detailed field information is available by pressing F1 on the DB2 region display panels or on any field in the display panels. Descriptions of DB2 region field names are also available in “DB2_REGION: DB2 subsystems” on page 1016.

A sample overview display panel for the DB2 region display report is shown in Figure 316 on page 424.

```
                DB2 region display                                Line 1 of 1
Command ===> ____________________________________________________ Scroll===> CSR
All DB2 region records                        6 Jun 2011 02:12
   Pri Jobname  Complex       System   LUNAME   SITENAME         DB2I GRPN RegU
__     DB9GMSTR EEND          SYS1     DB9GLU1  DALLAS9          DB9G
```

Figure 316. DB2 region overview display report

A sample detail display panel for the DB2 region display report is shown in Figure 317 on page 424.

```
                DB2 region display                                Line 1 of 36
Command ===> ____________________________________________________ Scroll===> CSR
All DB2 region records                        6 Jun 2011 02:12

Region identification
  Complex name                  EEND
_ System name                   SYS1
  DB2 System identification     DB9G
  DB2 Region job name           DB9GMSTR   Jobid  ASID 0036
  DB2 Region step name
  Local LU name                 DB9GLU1
   Local site name              DALLAS9
  Group attachment name
  Command character             -
  Linkage table index           00180100
  Region userid                                  Dfltgrp:

Region security settings
Classification Option       2 (1=single-subsystem, 2=multi-subsystem)
Class Name Root             DSN
Class Name suffix           1

SAF protection settings         Class    Act  Gen
Buffer pool privileges class    MDSNBP   Yes  Yes
Class system privileges         MDSNSM   Yes  Yes
Collection privileges class     MDSNCL   Yes  Yes
Stored proc privileges class    MDSNSP   Yes  No
Database privileges class       MDSNDB   Yes  Yes
Sequences class                 MDSNSQ   Yes  No
Java archive files class        MDSNJR   Yes  No
Table/index/view priv. class    MDSNTB   Yes  Yes
Package privileges class        MDSNPK   Yes  Yes
Tablespace privileges class     MDSNTS   Yes  Yes
Plan privileges class           MDSNPN   Yes  Yes
Schema privileges class         MDSNSC   Yes  No
User type privileges class      MDSNUT   Yes  No
Storage group privilege class   MDSNSG   Yes  Yes

Pri Audit concern
```

Figure 317. DB2 region detailed display report

Chapter 5. System Audit Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The system audit reports for monitoring z/OS using zSecure can be generated from

- "Interactive component zSecure Audit for RACF" explains how to start zSecure under ISPF and view system reports.
- "STATUS AUDIT - OVERVIEW" on page 430 describes the Status Audit Overview report.
- "STATUS AUDIT - MVS tables" on page 440 describes the system report types that do not require a full `CKFREEZE` data set read.
- "STATUS AUDIT - MVS extended tables" on page 499 describes the system report types that require a full `CKFREEZE` data set read.
- "AU.C Change track" on page 521 explains how to use the Change Track function to monitor changes in the security settings.
- "Batch auditing" on page 525 describes several ways to use zSecure for batch-only reporting.
- "Predefined CARLa scripts" on page 525 discusses the interactive ISPF and batch reports available in the SCKRCARL library.

Interactive component zSecure Audit for RACF

This section describes the system report types. Each report type description provides background information and report samples. See the following sections for more information:

- To start the product, see "Starting the interactive component" on page 9.
- For details on the zSecure ISPF panels, see "Panel structure" on page 10.

After you start the product, select the Audit option (AU) from the Main menu to open the Audit menu shown in Figure 318 on page 426.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
           zSecure Admin+Audit for RACF - Main menu
Option  ===> ____________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
  C    Change track    Track changes to the system
  L    Libraries       Library status and update analysis
  S    Status          Status auditing of security and system tables/options
  V    Verify          Verify and cleanup security database
RE   Resource        Resource reports
AM   Access          RACF Access Monitor
EV   Events          Event reporting from SMF and other logs
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex: Active primary RACF data base

Product/release:
5655-T01 IBM Security zSecure Admin 1.13.0
5655-T02 IBM Security zSecure Audit for RACF 1.13.0
```

Figure 318. zSecure Audit for RACF Main menu

This section of the documentation focuses on Audit functions. For more information on the Audit menu options, refer to the sections indicated in Table 197. For a table of references for the other main menu options like Events (EV) and RACF Administration (RA), see "Panel structure" on page 10. You can also find information about the panels and fields by using the context-sensitive help function available on most panels. To access the help, press PF1 or type HELP.

Table 197. Documentation references for Audit Menu options

Audit menu option	Documentation reference
AU.S Audit status	"STATUS AUDIT - OVERVIEW" on page 430 and "STATUS AUDIT - MVS tables" on page 440
AU.S, **RA** and **AU.V**	Information on the part of **AU.S** that pertains to a RACF audit and the menu options **RA** RACF and **AU.V** Verify is available inChapter 3, "RACF Audit Guide," on page 255.
AU.C Change Track	"AU.C Change track" on page 521
AU.L Libraries	Chapter 6, "Library Audit Guide," on page 529

The STATUS AUDIT application (option **AU.S** from the main menu) shows the contents of MVS and RACF security tables and settings. The first menu is displayed in Figure 319.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                          zSecure Audit - Audit - Status
Command ===> ____________________________________________________________
Enter / to select report categories
/    MVS tables      MVS oriented tables (reads first part of CKFREEZE)
/    MVS extended    MVS oriented tables (reads whole CKFREEZE)
_    RACF control    RACF oriented tables
_    RACF user       User oriented RACF tables and reports
_    RACF resource   Resource oriented RACF tables and reports

 Select options for reports:                                    Audit policy
 _   Select specific reports from selected categories          /  zSecure
 /   Include audit concern overview in overall prio order      _  C1
 _   Only show reports that may contain audit concerns         _  C2
 __   Minimum audit priority for audit concerns (1-99)        _  B1
 _   Print format              _  Concise (short) report
     _  Background run
```

Figure 319. Audit status menu

The available reports are divided into a number of categories. The first two, MVS TABLES and MVS EXTENDED, contain the pure MVS reports. The reports in the first category do not require a full CKFREEZE read, but the reports in the second category do. In addition, the RACF RESOURCE category contains a couple of reports that pertain mostly to MVS, but use RACF-specific knowledge on the protection of sensitive data sets, the protection of APF modules, the definition of started tasks, the relationship between RACF users and groups and z/OS UNIX UIDs and GIDs. The MVS categories are described in this chapter. The RACF categories are described in Chapter 3.

You can select categories by marking them with a '/'.

The panel allows you to specify the following processing parameters:

Select specific reports from selected categories
If you select this option, you will get a follow-up panel for each selected category where you can select the desired reports. If you do not select this option, all reports in the selected categories are generated.

Include audit concern overview in overall prio order.
This option determines whether an audit concern overview is generated. This overview shows up as the first item in the output. It is sorted by audit priority, and contains a single line for each item for which audit concerns were identified, including an indication of which report the item occurs in. Note that not all reports explicitly identify audit concerns; they are not represented here. The overview spans the categories selected (not just the selected reports). If you select this option without selecting any categories, an overview for all categories is generated. If you only want an overview across a specific category, you can select that category along with the *Select specific reports from selected categories* option, but not select any of the reports.

Only show reports that may contain audit concerns
If you select this option, only the reports that can contain audit concerns are displayed. If *Select specific reports from selected categories* is also requested, only the reports that can contain audit concerns are selectable.

Minimum audit priority for audit concerns (1-99)
Specify the minimum audit priority for audit concerns or leave blank for all records.

Print format
For a foreground run, selecting this option requests to present the output in a printable report format instead of as interactive displays. This is preferable if memory is tight or the output is to be printed. For a detail study of a small amount of data, the interactive display format is generally better suited. For a background run, this option has no effect.

Concise (short) report
Leave out detailed information from the generated reports. Use this option to review changes or explore the system. Do not use this option if you must have comprehensive audit information.

Background run
Submits a background (batch) job for generating the selected reports in print format. Selecting this option also implies that Print format is selected for the output. If you do not select this option, report processing runs in the foreground.

Audit policy
Select the audit policy for determining the audit concerns and priorities. The default audit policy raises the concern priority to 40 or more if it is likely that the system could almost certainly be compromised because of it. The *C1*, *C2*, and *B1* selections refer to the DoD orange book standards; these will also set priorities to 40 or more when a violation of the selected policy is noticed. It is not implied that all violations will be noted. In addition, *B1* will generate more audit concerns.

When running in foreground, Security zSecure displays the number of RACF and CKFREEZE records read during processing. After processing, the resulting output is displayed. Processing can be halted by pressing the ATTN key.

When you select certain reports, an additional panel opens for customizing the report. If you are running the reports for the first time to get a general overview, you can leave this panel blank.

When you have selected a set of system reports without selecting either *Output in print format* or *Run in background* , Security zSecure runs immediately and generates a report selection display showing the selected report information.

The contents of this display will of course vary with the report options selected. A sample report selection display is included in Figure 320 on page 429.

```
zSecure Suite Display Selection        1 s elapsed, 0.4 s CPU
Command ===> ____________________________________________________ Scroll===> CSR

 Name     Summary Records Title
_ SYSTEM         2       2 System settings and software levels
_ SYSTEMAU       2       8 System settings - audit concerns
_ IPLPARM        2       2 Effective system IPL parameters
_ SMFSUBOP       2       3 SMF subsystem-dependent settings
_ SUBSYS         1      61 Subsystem Communication Vector Tables
_ VSM            2      41 Virtual storage map
_ WRITABLE       1       1 Globally Writable Common Storage
_ MPFMSG         1     268 Message Processing Facility message intercepts
_ JOBCLASS       1      36 JES2 Job Class parameters (e.g. MVS command auth /
_ CONSOLE        1     114 Operator Consoles
_ PPT            1     114 Program Property Table
_ SVC            2     287 Supervisor Call Audit Display
_ PC             2    1595 Program Call Audit Display
_ TAPE           2       2 Tape protection settings (RACF)
_ IOAPPD         0       0 Authorized I/O Appendage table
_ IPSTACK        1       1 Communications Server IP stack display
_ IPPORT         1      35 Communications Server IP ports display
_ IPRULE         1       2 Communications Server IP rules display
_ IPVIPA         1       3 Communications Server IP VIPA display
_ IPINTFD        1       4 Communications Server IP interfaces display
_ IPROUTE        1       4 Communications Server IP routes display
_ IPNETACC       0       0 Communications Server IP netaccess display
_ IPAUTOL        1       2 Communications Server IP autolog display
_ IPRESOLV       1       1 Communications Server IP resolver display
_ DMS            0       0 DMS system settings
_ DMSAUDIT       0       0 DMS system settings - audit concerns
_ EXITS          2     112 Exit and table overview
_ DYNEXITS       1      77 Dynamic exit definitions
_ DASDVOL      230     230 DASD Volume Protection and Sharing
_ MOUNT          0       0 Effective UNIX mount points
_ SENSAPF        1     258 APF data set names
_ SENSLINK       1      46 Linklist data set names
_ SENSLPA        1      18 LPA list data set names
_ SENSALL        2     799 All sensitive data sets by priority and type
******************************** Bottom of Data ********************************
```

Figure 320. MVS Security report selection display

The preceding reports are based on the MVS system. They are described in this chapter. The reports based on RACF are described in Chapter 3.

zSecure Audit for RACF assigns a numerical *audit priority* to each system report entry, indicating the need to review the entry. Higher numbers indicate greater concern; numbers 20 and up require review, numbers 40 and up require immediate attention. In addition to the audit priority field each report entry also has an audit concern field which in case of a found concern describes the reason for the concern.

```
                                                                Line 86 of 499
Audit concern overview by priority (higher priorities only)
Command ===> _____________________________________________ Scroll===> CSR
                                          current settings
  Pri Complex  Syst Area Key         Audit concern
   20 NMPIPL87 IPO1 PORT   751   751 Because there is no SAF parameter, any u
   20 NMPIPL87 IPO1 SVC    83       Updated using SVCUPDTE, IBM-range SVCno,
   20 NMPIPL87 IPO1 SVC    95       Instruction scan hit, Caller may be unau
   20 NMPIPL87 IPO1 SVC   124       Code size suspect, Caller may be unautho
   20 NMPIPL87 IPO1 SVC   143       Updated using SVCUPDTE, IBM-range SVCno,
   15 NMPIPL87 IPO1 HSM  ERASEONS  N Disk scavenging threat not countered in
   13 NMPIPL87 IPO1 PC   TN3270   00 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   01 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   02 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   03 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   04 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   05 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   06 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   07 In caller's private area, Executes autho
   13 NMPIPL87 IPO1 PC   TN3270   08 In caller's private area, Executes autho
```

Figure 321. MVS Security audit overview display

STATUS AUDIT - OVERVIEW

The OVERVIEW report at the top of the selection list is a good point to start a system audit. The report summarizes the most important audit concerns across all report types and all systems audited, sorted by numerical audit priority. A pointer to the relevant report type is included. We suggest you view this report first, and then explore the other reports, starting with the reports having the highest audit priority. Figure 322 shows an audit overview display.

Figure 322. MVS Security audit overview display

The overview report contains the following fields of interest:

Table 198. Audit concern overview by priority - field descriptions

Field	Explanation
Pri	Numerical audit priority, identifying the severity of the problem. Priorities of 40 and up indicate a very serious concern, requiring immediate attention. Priorities in the range 20 to 39 require review because serious security threats might exist.
Complex	The name of the complex to which the system belongs on which audit concerns were identified.
Syst	The name of the system on which the audit concern was identified.
Area	The report type in which the audit concern was identified.
Key	The report key identifying the entry within the relevant report. The value and meaning of the key is report dependent.
Audit concern	The audit concern identified. Background information on the reason for the concern.

The table lists the abbreviations and the NEWLIST types for the various report types. The page numbers refer to the audit concern sections.

Table 199. NEWLIST type abbreviations listed by report type

Abbreviation	Report type	NEWLIST type
CLAS	Class Descriptor Table	CLASS (page 990)
CONS	Console	CONSOLE (page 1004)
DASD	DASD volume	DASDVOL (page 1013)
DMS	SAMS:Disk parameters	AUDIT (page 961)
EXIT	Exit	EXIT (page 1029)
FILE	UNIX files	UNIX (page 1481)
HSM	Hierarchical Storage Manager	AUDIT (page 961)
IOAP	I/O appendage	IOAPP (page 1052)
IP	IP stack	IP_STACK (page 1075)
IPRE	IP resolver	IP_RESOLVER (page 1066)
JCL	JES2 job class	JOBCLASS (page 1090)
MOUN	UNIX Mount Points	MOUNT (page 1104)
MSG	Message Processing Facility	MSG (page 1107)
MVS	MVS properties	AUDIT (page 961)
PC	Program Call	PC (page 1113)
PORT	IP port	IP_PORT (page 1061)
PPT	Program Property Table	PPT (page 1122)
RACF	RACF profiles	RACF (page 1131)
ROUT	SAF router table	ROUTER (page 1250)
SENP	Sensitive profiles	REPORT_SENSITIVE (page 1242)
SENS	Sensitive data sets	SENSDSN (page 1256)
SETR	SETROPTS settings	AUDIT (page 961)
SMF	SMF system settings	AUDIT (page 961)
SMFO	SMF subsystem	SMFOPT (page 1403)
SSCT	Subsystem	SUBSYS (page 1407)
STOR	Writable common storage	CSM (page 1009)
SVC	SuperVisor Call	SVC (page 1417)
SYSL	Syslog settings	AUDIT (page 961)
TRUS	Trusted users and sensitive resources	(page 1476)
TSO	TSO settings	AUDIT (page 961)
VM	VM properties	AUDIT (page 961)
VSM	Virtual storage map	VSM (page 1493)

Each of these types is described in this guide. See Chapter 3, “RACF Audit Guide,” on page 255 for a description of CLAS, FILE, RACF, SENP, SETR and TRUS.

If you select one of the audit concerns listed with the **S** action character, a detail display is shown.

```
Audit concern overview by priority (higher priorities only)       Line 1 of 17
Command ===> ____________________________________________________ Scroll===> CSR_
                                          29 Aug 2000 00:07

System
Complex name                  RULELINE
System name                   0250

Audit concern

Relative audit priority       27
Audit concern                 Updated without SVCUPDTE, Reserved SVCno, In
Audit concern                 (E)CSA/(E)SQA, Caller may be unauthorized

SVC
SVC number                     28
ESR number
Current SVC requires APF      No
Default function of the SVC
SVC residency                 CSA
SVC entry point at
****************************** Bottom of Data ********************************
```

Figure 323. Detail display layout (for an SVC concern)

The detail display layout depends on the report type in which the audit concern was identified, the preceding example shows the layout for an SVC concern.

The detail display repeats the following report-independent fields of interest (in full):

Table 200. Audit concern overview by priority detail view - field descriptions

Field	Explanation
Complex name	The complex name
System name	The system name
Relative audit priority	The severity of the concern
Audit concern	The audit concern identified

The detail display also contains a report-dependent section, containing the fields mentioned in the following tables. See Chapter 3, "RACF Audit Guide," on page 255 for the explanation of CLAS, FILE, RACF, SENP, SETR, and TRUS details.

Table 201. Audit concern overview by priority detail view - Console report field descriptions

Field	Explanation
Console number	The console number.
Console name	The console name.
Device number	The console's device number. This field is not present for subsystem consoles.
Job or subsystem name	The subsystem the console is dedicated to, or the jobname for EMCS consoles. In other cases, this field is blank.
Console logon	The system-wide setting that determines whether logon is required to use a console. It can be *OPTIONAL*, *REQUIRED*, or *AUTO*.
User logged on to console	The user ID logged on to the console. This field is blank if no one is logged on to the console (when the previous field shows *OPTIONAL*).

Table 201. Audit concern overview by priority detail view - Console report field descriptions (continued)

Field	Explanation
Command authority	Indicates the types of commands that can be issued from the console. This field can have one or more of the following values: *SYS* (system) *IO* (I/O) *CONS* (console) *MASTER* (master console) *INFO* (informational) *ALL* (all of these)
Undirected messages	Whether this console accepts undirected messages.
Routing codes	The routing codes for this console.
Message level	The kind of messages the console accepts. It can contain any combination of the following values: • *R* (requiring operator reply) • *I* (immediate action) • *CE* (critical event) • *E* (event) • *IN* (informational) • *NB* (no broadcasts) • *ALL* (all of these)
Alternate console name	The name of the alternate console (if any). On older MVS releases (earlier than SP4.1) this field contains the device number of the alternate console instead of its name.

Table 202. Audit concern overview by priority detail view - DASD volume report field descriptions

Field	Explanation
Volume serial	The DASD volume's volume serial number.
DASD box serial number and id	The box serial number consisting of manufacturer id, factory id and serial number, plus the device id associated with it.
DASD box type	The DASD type, followed by the model.
Number of systems mounted	The number of systems that the volume is mounted on.

Table 203. Audit concern overview by priority detail view - SAMS:Disk field descriptions

Field	Explanation
Parameter name	The SAMS:Disk parameter
Parameter value	The value the parameter is set to.

Table 204. Audit concern overview by priority detail view - Exits and table field descriptions

Field	Explanation
Application owning exit	The application or subsystem owning the exit.

Table 204. Audit concern overview by priority detail view - Exits and table field descriptions (continued)

Field	Explanation
SMF subsystem using exit	The subsystem name (when the previous value was JES2).
Name of the dynamic exit	Full name if it is a dynamic exit, blank otherwise.
Function of the exit	A description explaining the exit's function.
Exit program name	The documented program name of the exit or table.
Jobname of exit address space	The jobname of the address space the exit resides in, if in (E)PVT.
Exit address at	A description of program name or module name, and offset.
Address called for the exit	For an exit the entry point, for a table its start address.
Exit length	The length of the program/module the exit is a part of
Exit residency	The virtual storage area where the exit resides.
Exit storage area key	The storage protection key of the exit or table.
Exit storage area subpool	The storage area subpool, if in (E)CSA or (E)SQA.

Table 205. Audit concern overview by priority detail view - HSM / MVS / SMF / SYSL / TSO - System settings field descriptions

Field	Explanation
Parameter area	The area of concern: HSM (Hierarchical Storage Manager), MVS, SYSLOG (system log), SMF (audit log), or TSO.
Parameter name	The system parameter.
Parameter value	The value it is set to.

The report type "SMF" can also refer to the "SMF subsystem" report. See “SMFSUBOP - SMF subsystem report” on page 446.

Table 206. Audit concern overview by priority detail view - I/O appendage (IAOP) field descriptions

Field	Explanation
Appendage ID	The id of the authorized I/O appendage.
Appendage type	The I/O appendage is one or more of the following types: *ABE* (abnormal end), *CHE* (channel end), *EOE* (end of extent), *PCI* (program controlled interrupt), *SIO* (start I/O).
Conforms to default	Whether the types enumerated above accord to the IBM default
Appendage description	A description of the function of the I/O appendage.
Module name loaded by OPEN	The full name of the I/O appendage (always starts with IGG019).
Entry point if resident	The address in-storage, if loaded.

Table 206. Audit concern overview by priority detail view - I/O appendage (IAOP) field descriptions (continued)

Field	Explanation
Appendage residency	The virtual storage area where the appendage resides

Table 207. Audit concern overview by priority detail view - IP port report field descriptions

Field	Explanation
Beginning port	The first port in a range of reserved ports.
End port	The last port in a range of reserved ports.
Bind IP address	The IP address associated with the job name present in the JOBNAME field.
Port use restriction	An indication of how the port is used.
Port count	The number of ports in a range of reserved ports.
Port options	Information about the current status of IP interface settings.
PORTRANGE entry	Indication whether a PORTRANGE statement was used.
Protocol	The protocol associated with a range of ports.
Secure unreserved ports	Indication whether a PORT UNRSV statement was used.
SERVAUTH resource name	The name of a SAF SERVAUTH resource.

Table 208. Audit concern overview by priority detail view - IP resolver report field descriptions

Field	Explanation
Stack name	The member name of the procedure used to start the TCP/IP address space.
Host name	The TCP host name of the z/OS CS server.
Setup file	The name of the resolver setup file name (either an MVS data set or a z/OS UNIX file) that contains resolver configuration statements.
Default TCPIP.DATA file	The name of either a z/OS UNIX file or MVS data set with TCPIP.DATA statements that is the last file that is searched by the resolver for resolver configuration information.
Global TCPIP.DATA file	The name of either a z/OS UNIX file or an MVS data set containing the statements that define the global TCPIP.DATA settings for the entire MVS image and for all TCP/IP stacks.
Default IPNODES file	The name of either a z/OS UNIX file or MVS data set that contains the hard-coded IP addresses and host names to be used.
Global IPNODES file	The name of either a z/OS UNIX file or MVS data set that contains hard-coded IP addresses and host names that are used globally.

Table 209. Audit concern overview by priority detail view - IP stack report field descriptions

Field	Explanation
Stack name	The stack name which is the name of the started task procedure running the stack.

Table 209. Audit concern overview by priority detail view - IP stack report field descriptions (continued)

Field	Explanation
TCP low ports restricted	Flag field that indicates whether TCP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements.
UDP low ports restricted	Flag field that indicates whether UDP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements.
Start date/time	The date and time that the TCP/IP stack was started.
Last change date and time	The date and time that the TCP/IP stack was last changed.
Dataset name (member)	This repeated field contains an entry for each profile information data set name followed by a member name between brackets: [membername]. The data set name entries can originate from the following sources: an OBEYFILE command, the default library found in the standard search sequence, or an INCLUDE statement.
TCP/IP stack source VIPA	The IPv4 address used as the source IP address for outbound TCP connections.
VIPA interface name (IPv6)	The name of a static VIPA or a dynamic VIPA interface.

Table 210. Audit concern overview by priority detail view - JES2 job class (JCL) field descriptions

Field	Explanation
Subsystem name	The name of the subsystem.
Job class	The class name (a single character).
Command disposition	The action taken for MVS commands embedded in JCL: DISPLAY (display on the console and execute without verification), EXECUTE (execute without display or verification), IGNORE (silently ignore the command), or VERIFY (have the operator verify the command).
Authorized command groups	The MVS command groups to be executed: any combination of SYS (system), IO (I/O), CONS (console) and INFO (informational), or ALL (all of these).
Bypass Label Processing	Whether the bypass label parameter in the label field of a DD parameter is performed subject to SAF controls (vs. ignored entirely).
Jobs held until released	Whether jobs in this class are held until the operator issues a RELEASE.

Table 211. Audit concern overview by priority detail view - UNIX mount points (MOUN) field descriptions

Field	Explanation
Mount point	The absolute pathname of the mount point
Unix device number	The device number as assigned when the file system is mounted.
File system mode	The mode in which the file system is mounted: READ (read only) or RDWR (read/write)
File system type	The type of the file system (AUTOMNT,TFS,HFS,ZFS,.....)

Table 211. Audit concern overview by priority detail view - UNIX mount points (MOUN) field descriptions (continued)

Field	Explanation
File system name	The name of the file system.
Mounted with security	Whether the file system is mounted with the security attribute. If not, any user can access and change any file in it.
Mounted with SETUID	Whether the file system is mounted with the SETUID attribute. If not setuid, setgid, APF and program control attributes are not honored.
File system supports ACLs	Whether the filesystem supports access lists.
New block security	Whether blocks that are allocated are cleared before they are linked.
Owning complex	The complex the "Owning system" is in.
Owning system	The system that owns the file system.
Data set name	The name of the MVS data set that contains the file system.
Volume serial	The volume serial that holds the MVS data set.
DASD box serial number and ID	The serial code of the volume containing the code of the manufacturer, factory code, box serial number, and device tag.
Size of block in bytes	Size of a block of the zFS file system in bytes (normally 8192).
Size of fragment in bytes	Size of a fragment of the zFS file system in bytes. Multiple files can share a logical block if they are smaller than (block size - fragment size), in which case the block gets split up in fragments. The size of a fragment can range from 1024 up to the block size.
Size of aggregate in blocks	The size in blocks of the aggregate. Normally the number of blocks that fit in the primary allocation.

Table 212. Audit concern overview by priority detail view - Message Processing Facility (MSG) field descriptions

Field	Explanation
Message id	The message id
Suppress message	Whether the message is suppressed.
Automation for messages	Whether the message is automated; if so, and if an automation token was defined, that token is shown.
Parmlib member	The parmlib member used to set MPF processing for this message.
Exit name	The module name of a user exit for this message (if any).
Exit address	The address of the user exit.
Exit residency	The virtual storage area where the exit resides.
Exit load module information	The program name, module name and offset for the exit.

Table 213. Audit concern overview by priority detail view - Program call (PC) field descriptions

Field	Explanation
Entry Table owning jobname	The jobname of the address space owning the Entry Table.
Entry Index	The index in the Entry Table that identifies the program call routine
Function Description	If system-wide, a description of the entry in the System Function Table. Otherwise, the value might contain the best guess for the description as determined by Security zSecure processing based on the module name. If the value represents a guess, it is enclosed in brackets to indicate uncertainty.
Authority required	Whether authority (not key 8) is required to call the routine.
PC routine residency	The virtual storage area where the program call routine resides.
Program Call entry point at	The program name, module name and offset for the program call routine.

Table 214. Audit concern overview by priority detail view - Program Property Table (PPT) field descriptions

Field	Explanation
Program name (must be APF)	The program name that gets properties assigned (if APF)
Job step storage key	The key in which the program runs (if assigned); key 0 to 7 imply system authorization
Bypass password / SAF	Whether DFSMS will bypass invoking SAF for security checks by the External Security Manager (RACF).
No data set integrity	Whether no enqueues are done for data sets in the batch. If enqueues are not done, it might cause problems with data management procedures that result from a data set being removed while it is being used.
Default entry IEFSDPPT	Whether this entry comes from the default module IEFSDPPT, and not from SCHEDxx.
Non-swappable	Whether the program is non-swappable.
Non-cancellable	Whether the program cannot be cancelled with a CANCEL command.
Privileged (no SWAP)	Whether the program runs privileged; if so the program is not swapped unless it is in a long wait state.
System task not timed	Whether the program is a system task, and not timed.

Table 215. Audit concern overview by priority detail view - SAF Router Table (ROUT) field descriptions

Field	Explanation
Class name	The class name passed to the RACROUTE call.
Requestor name on RACROUTE	The requestor name passed to the RACROUTE call.
Subsystem name on RACROUTE	The subsystem name passed to the RACROUTE call.

Table 215. Audit concern overview by priority detail view - SAF Router Table (ROUT) field descriptions (continued)

Field	Explanation
Action (NONE or RACF)	The action to be taken for this requestor, class, and subsystem. 'NONE' indicates RACROUTE requests are to be ignored (RC=0), 'RACF' indicates RACF is to be called.

Table 216. Audit concern overview by priority detail view - Sensitive data sets (SENS)

Field	Explanation
Type of sensitive data set	The sensitivity type of the data set.
Data set name	The name of the data set.
Volume serial	The volume serial of the data set.
Access level that is exposure	The access level considered an exposure for this sensitivity type

Table 217. Audit concern overview by priority detail view - SMF subsystem (SMFO)

Field	Explanation
SMF subsystem name	The name of the subsystem for which the SMF options are set.
Summary of recording activity	A line describing what SMF records are suppressed and which are written

Note that the report type "SMF" can also refer to "System settings". See Table 205 on page 434.

Table 218. Audit concern overview by priority detail view - Subsystem (SSCT) field descriptions

Field	Explanation
Subsystem name	The subsystem name.
Subsystem type	The subsystem type (JES2, JES3, or blank)
Functional description	The name of the package normally creating this subsystem (if known to Security zSecure).

Table 219. Audit concern overview by priority detail view - Common storage (STOR) field descriptions

Field	Explanation
Storage area type	The virtual storage area type: (E/X)CSA or (E)SQA.
Storage area key	The storage protection key of the area.
Storage area subpool	The storage area subpool.
Start address	The start address of the storage area.
End address	The end address of the storage area
Length of storage area	The length of the storage area.

Table 220. Audit concern overview by priority detail view - Supervisor call (SVC) field descriptions

Field	Explanation
SVC number	The SVC number.
ESR number	For an extended SVC, the Extended Supervisor Router table index.
Current SVC requires APF	Whether the SVC requires the caller to be authorized.
Default function of the SVC	The function of the SVC; if shown in brackets, a guess based on the entry point name.
SVC residency	The virtual storage area where the SVC resides.
SVC entry point at	A description of the SVC's program name, module name and offset.

Table 221. Audit concern overview by priority detail view - Virtual storage (VSM) field descriptions

Field	Explanation
Storage area type	The virtual storage area type.
Start address	The start address of the storage area.
End address	The end address of the storage area.
Length of storage area	The length of the storage area.
% Area in use	For (E)CSA, the percentage used.

The system report types generally have the same structure: a summary by system, an overview display, and a detail display. The overview display is sorted by descending audit priority, listing the most important entries first. In an overview display, the important audit concerns are in the rightmost column.

STATUS AUDIT - MVS tables

The z/OS system report types available in zSecure Audit do not require a full CKFREEZE data set read. For each report type, the background is discussed, and sample displays or batch report output is presented and discussed.

These reports are available in batch mode, and under ISPF from the STATUS AUDIT MVS TABLES.

Note: In general, running the latest version of zSecure Collect APF-authorized results in the most detailed reports. Older versions and non-APF runs typically result in missing information.

The following system reports are available:

SYSTEM - MVS system settings report

The MVS system settings display shows an integrated display of MVS system parameters, system software levels, and settings. The amount of information available is increased if a later version of zSecure Collect is used or if zSecure Collect is run authorized.

This report is available on a live system; no CKFREEZE file is required.

For documentation on each of the fields displayed and the audit considerations involved, refer to the language reference for the NEWLIST TYPE=SYSTEM in Chapter 13, "SELECT/LIST Fields," on page 953. Furthermore, a second report SYSTEMAU shows the audit concerns. The audit concern report is part of the system settings report, but can also be run directly from CARLa scripts CKADSY80 (display), CKALSY80 (list, 80 characters wide) and CKALSY13 (list, 132 characters wide).

For more information on system audit concerns, see the description of AUDITCONCERN in AUDIT: System setting audit concerns "AUDITCONCERN" on page 961.

Figure 324 on page 442 shows the MVS system setting display.

```
System settings and software levels                              Line 1 of 67
Command ===> ____________________________________________ Scroll===> CSR
                                          9 Dec 2005 00:07
    Complex  System   Sysplex  SC Nodename VTAM net HwName   ConfigID LPAR     L
    SYS1     IPO1     PLEX1    87 NMS87    USIBMNT  VM-TOKEN GUEST            0

System identification                 Configuration parameters
Sysplex name                 DINORD2R MVS load parameter           2030AAM
Hardware name                M3000H30 Initial Program Load device  2016
Logical Partition name       PROD     Initial Program Load volume  Z140R1
Virtual machine userid                MVS I/O configuration id     09
VM system name                        Initial Program Load date    Friday
JES node name                JES2DINO Initial Program Load date    29Apr2005
VTAM net identifier          NLCRMM04 Initial Program Load time    17:14
Time zone relative to GMT    +01:00   IODF configuration id        OS390
CPU processor type           7060     IODF configuration date      09Dec2004
CPU processor model byte     1C       IODF configuration time      12:31
CPU serial (starts with LPAR) 213FF   &SYSCLONE, short for SYSNAME  XX
CPU model name               IBM 7060 model P30

Software levels
Operating system vendor      IBM CORP
Operating system             z/OS
OS   Operating system version 1.4.0
ESM External Security Manager RACF HRF7707 OA03853

MVS level                    SP7.0.4
JES  Job Entry Subsystem     z/OS 1.4
SMS  System Managed Storage  DFSMS 1.3.0
DFP  Data Facility Product   3.3.2
HSM  Hierarchical Storage Mgr 1.5.9
TSO  Time Sharing Option     3.3.0
VTAM Virtual Terminal Acc Fac 6.1.4/ESA
TCP/IP procedure & version   TCPIP    TCP/IP CS for z/OS V1R4
RMF  Resource Measurement Fac 7.1.2
VM   Virtual Machine

Console and MPF options               SYSLOG/hardcopy log
Console message loss         No       System log active            Yes
CONSOL suffix                A0       System log SYSOUT class      L
MPFLST suffix                         System log SYSOUT limit        5000
PFKTAB suffix                00       Monitor dsname active        Yes
Console command delimiter    "        Monitor space active         No
Console logon required       No       Events to be monitored
Console logon automatic      No       Hardcopy device              SYSLOG
AMRF retention active        Yes      Hardcopy command level       CMDS
UEXIT IEAVMXIT active        No       Hardcopy routecodes          1:128
Default routecodes           1:128
MLIM WTO buffer limit        6000
RLIM WTOR buffer limit         99

SMF parameters                        MVS and DFP options
Current SMFPRM suffix                 Multi Level Alias qualifiers   1
SMF recording active         Dataset  All linklist authorized      Yes
Max Job Wait Time    HH:MM    03:00   All REFR pgms Key 0  REFRPROT
Max SMF not yet on disk MM:SS   30:00 Jobcat / stepcat enabled     Yes
SMF 23/status each   HH:MM:SS 01:00:00
SMF 17/scratch also temp dsn  No      TSO parameters
Halt sys if SMF buffers full  No      Current TSO parameter source IKJTSO00
Halt sys if last SMF dataset  No      TSO maximum number of users     50
SMF restart after dump abend  Yes     TSO maximum reconnect minutes   10
Dflt 64bit MEMLIMIT(MB)               TSO ACB password present     No
                                      Encrypt TSO/VTAM buffers     Yes

SMF recording data set                Volume    Size  Blocks  %U Active
DINO.MAN1                             DINOSY   28800    7200   8 Yes
DINO.MAN2                             DINOSY    7200    1800   0 No
DINO.MAN3                             DINOSY    7200    1800   0 No

SMF log stream              Df1 Bufsize Act Con Recording Activity summary

HSM job  Migr pfx Bkup pfx RACFind BkupProf MulTpVol TpSelVol Erase SMF
DFHSM    DFHSM    DFHSM    No      Yes      No       No       No    240
****************************** Bottom of Data ********************************
```

Figure 324. MVS system settings display

The MVS system settings audit concerns report SYSTEMAU shows the audit concerns identified.

The following figure shows a sample MVS audit concerns summary display.

```
System settings - audit concerns                                  Line 1 of 2
Command ===> ____________________________________________________ Scroll===> CSR
                                                 1 Sep 2000 00:07
   Pri Complex  System   Count
    15 DEFAULT  DINO         3
   Pri Area     Count
__  15 HSM           1
s_   5 SMF           2
****************************** Bottom of Data ********************************
```

Figure 325. MVS audit concerns summary display

The display contains the following fields of interest.

Table 222. System settings audit concerns - field descriptions

Field	Explanation
Pri	The highest priority for any audit concern for this system
Complex	The complex name
System	The system name
Count	The number of audit concerns for this system
Pri	The highest priority for the area
Area	The area of concern (HSM, MVS, SMF, SYSLOG or TSO)
Count	The number of audit concerns in the area

Select one of the areas to obtain a display of the audit concerns in it.

```
System settings - audit concerns                                  Line 1 of 2
Command ===> ____________________________________________________ Scroll===> CSR
                                                 1 Sep 2000 00:07
   Pri Complex  System   Count
    15 DEFAULT  DINO         3
   Pri Area     Count
     5 SMF           2
   Pri Parameter                Value    Audit concern
s_   5 LASTDS                   No       Hacker can work unobserved after flood
__   5 NOBUFFS                  No       Hacker can work unobserved after flood
****************************** Bottom of Data ********************************
```

Figure 326. MVS audit concerns display

The display contains the following fields of interest.

Table 223. System settings audit concerns detail view - field descriptions

Field	Explanation
Pri	A measure for the severity of the audit concern
Parameter	The system parameter that causes the audit concern
Value	The value the parameter is set to
Audit concern	The audit concern identified for this setting

Select an audit concern for a detail display.

```
System settings - audit concerns                                Line 1 of 14
Command ===> ____________________________________________ Scroll===> CSR
                                          1 Sep 2000 00:07

System
Complex name                  DEFAULT
System name                   DINO

System setting
Parameter area                SMF
Parameter name                LASTDS
Parameter value               No

Audit concern
Relative audit priority       5
Audit concern                 Hacker can work unobserved after flooding audit
Audit concern                 trail / not C2 compliant
****************************** Bottom of Data ********************************
```

Figure 327. MVS audit concerns detail display

The detail display shows no additional information.

IPLPARM - IPL parameters report

The IPL parameters display shows the effective values of the IPL parameters (of the last IPL), the effective values of the LOADxx member that was used (with the volume serials for PARMLIB statements resolved), but first of all lists the operator-specified IPL parameters.

This report is available on a live system (no CKFREEZE file is required).

Documentation for each of the fields displayed, and the audit considerations involved, can be found in the language reference for SYSTEM NEWLIST in Chapter 13, “SELECT/LIST Fields,” on page 953. For detail information on the IPL parameters specified in IEASYSxx and the statements in LOADxx, refer to the sections in the Initialization and Tuning Reference on these parmlib members.

```
Effective system IPL parameters                                  Line 1 of 101
Command ===> ____________________________________________ Scroll===> CSR_
                                                          21 Aug 2008 13:58
   Complex  System   Collect time stamp
   EEND     EMOS     21 Aug 2008 13:58

 Operator-specified IPL parameters
 SYSP=(00,3A)

 Security related flags
 Prompt operator at IPL    OPI Yes
 Linklist authorized   LNKAUTH Yes
 Create Link Pack Area    CLPA Yes
 Clear VIO                CVIO
 Master JCL from linklib       No
 LOADxx PARMLIBs used          Yes

 Suffix parameters
 IEASYSxx suffixes        SYSP (00,3A)
 ALLOCxx suffixes        ALLOC 00
 IEAAPFxx suffix           APF
 AUTORxx suffixes        AUTOR
 AXRxx suffixes            AXR 00
 CEEPRMxx suffixes         CEE
 CLOCKxx suffix          CLOCK 00
 COMMNDxx suffixes         CMD (30)
 CONSOLxx suffix           CON (30,NOJES3)
 COUPLExx suffix        COUPLE 30
 DEVSUPxx suffixes      DEVSUP
 DIAGxx suffixes          DIAG 00
 EXITxx suffixes          EXIT
 IEAFIXxx suffixes         FIX
 GRSCNFxx suffix        GRSCNF 00
 GRSRNLxx suffixes      GRSRNL
 IEAICSxx suffix           ICS
 IKJTSOxx suffix        IKJTSO 00
 IECIOSxx suffix           IOS
 IEAIPSxx suffix           IPS 00
 LNKLSTxx suffixes         LNK 00
 LPALSTxx suffixes         LPA (30)
 LPALSTxx suffixes         LPA (30)
 IEALPAxx suffixes        MLPA (00)
 MSTJCLxx suffix       MSTRJCL 00
 BPXPRMxx suffixes        OMVS (30)
 IEAOPTxx suffix           OPT (30)
 IEAPAKxx suffixes         PAK 00
 IFAPRDxx suffixes        PROD (30,3A)
 PROGxx suffixes          PROG (00,30,0A)
 CSVRTLxx suffix          RTLS
 SCHEDxx suffixes          SCH 00
 SMFPRMxx suffix           SMF 00
 IDGSMSxx suffix           SMS 00
 IEFSSNxx suffixes         SSN (00,0A)
 IEASVCxx suffixes         SVC 00
 CUNUNIxx suffix           UNI
 VATLSTxx suffixes         VAL 30
```

Figure 328. IPL parameters display

```
Effective system IPL parameters                                  Line 57 of 101
Command ===> ____________________________________________ Scroll===> CSR_
                                                          21 Aug 2008 13:58
 Complex  System   Collect time stamp
 EEND     EMOS     21 Aug 2008 13:58


 Various
 System name           SYSNAME
 Sysplex configuration PLEXCFG MONOPLEX
 Channel Measurement Blks  CMB
 Disaster Recovery      DRMODE
 SYS1.DUMPxx data sets    DUMP DASD
 Global Resource Serializ. GRS NONE
 License               LICENSE z/OS
 Max concurrent jobs   MAXUSER 255
 Rsvd sys link indexes  NSYSLX 165
 Use all present CPUs  PRESCPU
 Reliability Data Extract. RDE No
 Reduced Error Recovery    RER No
 Non-reuse. ASVT entr. RSVNONR 5
 STC-rsvd ASVT entries RSVSTRT 5
 ZAAP work on ZIIP    ZAAPZIIP Yes
 Logging parameters
 Systemlog SYSOUT class LOGCLS L
 Systemlog SYSOUT limit LOGLMT   5000
 Logrec record. medium  LOGREC IGNORE

 Storage
 Common Service Area sizes CSA (1000,40000)
 CSCB Location         CSCBLOC ABOVE
 High virt shared area HVSHARE 510T
 Common area          HVCOMMON 64G
 Real back stor pages   LFAREA 0M
 Max SCOPE=COMMON dspcs MAXCAD 50
 Max amount centr storage REAL 76
 Reconfig. System Units    RSU 0
 System Queue Area sizes   SQA (1024K,1024K)
 Virtual=Real dflt regn VRREGN 64

 Page/swap information
 Max page/swap d.sets  PAGTOTL (9)
 DUPLEX paging data set DUPLEX
 VIO journaling DS Name VIODSN IGNORE
 Page data sets no VIO  NONVIO
 IEASYSxx page data sets  PAGE PAGE.EMOS.PLPA PAGE.EMOS.COMMON PAGE.EMOS.LOCAL1
 Operator page data sets
 Swap data sets           SWAP

 Effective LOADxx cards
 IODF     03 SYS1     MVS1
 SYSPARM  (00,3A)
 SYSCAT   EMOSSY113CCATALOG.MASTER.EMOS
 IEASYM   (00,L)
 SYSPLEX  EMOSRD2R
 PARMLIB  SYS1.PARMLIB                                  EMOSSY
 PARMLIB  SHARED.PARMLIB                                SHR001
 PARMLIB  SYS1.PARMLIB.INSTALL                          A1A0R1
 PARMLIB  SYS1.PARMLIB.POK                              A1A0R1
 ******************************** Bottom of Data ********************************
```

Figure 329. IPL parameters display (continued)

SMFSUBOP - SMF subsystem report

The SMF subsystem report checks whether the SMF record types most relevant for auditing are written, and generates an audit concern accordingly.

This report is available on a live system (no CKFREEZE file is required).

Background

SMF options can be set system-wide, and per subsystem. Each subsystem can be controlled separately. In addition, the pseudo-subsystems STC (for started tasks) and TSO (for interactive TSO users) can be specified. The default options for any subsystem not explicitly present are listed under the subsystem name *SYS*.

The system-wide options include the following:

- The action to take when SMF runs out of disk data sets or buffers: either lose records, halt the system or wait the system until space is available.
- The SMF recording data sets.
- Whether or not to write SMF record type 17 (scratch data set) for temporary data sets.
- The time-interval between the writing of subsequent SMF record types 23 (SMF Statistics).

These options are reported in the MVS system settings report (AU.S, MVS tables, SYSTEM). See also "SYSTEM - MVS system settings report" on page 441.

The options that can be set per subsystem include:

- The SMF records that are written to SMF.
- For each SMF record type, the subtypes that are written to SMF.
- The SMF exits that are active. (The exit IEFU83 for instance can be used to suppress SMF records independently of the recording activity settings.)

The information in the SMF subsystem report is based on in-storage SMF control blocks and is available both from the CKFREEZE file and from the current settings.

The SMF parameters are specified in parmlib member SMFPRMxx.

Auditing SMF subsystem settings

The following considerations apply when auditing SMF subsystems:

- Check the exits that are called for each subsystem.
- Check that SMF 7 is written. This record type indicates that SMF records were lost because the buffers or recording data sets were full, for example. If your system loses SMF records and does not write SMF 7, the loss of data is undetected.
- Check that the security related SMF records are written. For RACF: SMF 80 and 81, for Top Secret SMF 80 and for ACF2 is site definable (default is SMF 230). The RACF, ACF2 or Top Secret SMF records should not be suppressed. If you have RACF and MLACTIVE is set, or use other products that write SMF 83 records, SMF 83 should also be written.
- Check that either SMF 20 or SMF 30-1 is written. If neither is written, job starts are not logged. Note that RACF does not log all job starts.
- Check that SMF 14-15, 17-18, 60-62, and 64-67 are written. These records describe data set activity.
- If long-running jobs need to be accounted, check that interval recording is active.

The batch report to review the SMF subsystems is CKALSMFS. The interactive report is called CKADSMFS.

Figure 330 on page 448 shows a sample SMF subsystem overview display.

```
SMF subsystem-dependent settings                                  Line 1 of 9
Command ===> _____________________________________________ Scroll===> CSR_
                                              12 Oct 1994 02:10
   Complex  System   SMF subsystems Audit concerns Priority
   SMFS@510 ML1E                 9              5       29
   Pri Subs Su# Wr# Pa# Ex# Det Interval Recording activity summary
__ 29 RCT4 253   1   2   1 No  00:15:00 Write 100(5:8) 101(1,2,8:10) 102
__ 29 RCT5 254   2   0   1 No  00:15:00 Write 32 40
__ 29 RCT6 252   2   2   1 No  00:15:00 Write 100(5:8) 101(1,2,8:10) 102:103
s_ 29 RCT7 252   1   3   1 No  00:15:00 Write 100(5:8) 101(1,2,8:10) 102 103(64
__  5 STC   14 242   0   6 No  00:15:00 Suppress 14:19 62:69
__    RCT1   1 253   2   1 No  00:15:00 Suppress 100(5:8) 101(1,2,8:10) 102
__    RCT2   2 254   0   1 No  00:15:00 Suppress 32 40
__    RCT3   2 254   0   1 No  00:15:00 Suppress 32 40
__    SYS    0 256   0  12 Yes 00:15:00 Write 0:255
******************************* Bottom of Data ********************************
```

Figure 330. SMF Subsystem Overview Display

The overview display contains the following fields of interest:

Table 224. SMF Subsystem Overview Display - field descriptions

Field	Explanation
Complex	The complex name.
System	The system name.
SMF subsystems	The number of SMF subsystems.
Audit concerns	The number of SMF subsystems for which audit concerns were identified.
Priority	The highest audit priority found for any of the SMF subsystems.
Pri	The audit priority for the individual SMF subsystem.
Subs	The subsystem name.
Su#	The number of record types completely suppressed.
Wr#	The number of record types completely written.
Pa#	The number of record types partly suppressed, partly written.
Ex#	The number of exits defined.
Det	Indicates whether detail recording is active.
Interval	Indicates the recording interval time.
Summary	A summary of the record types suppressed and written.
Audit concern	Identified audit concerns.

Select any subsystem for a detail view, showing the active exits for this subsystem, and the SMF records being written.

```
SMF subsystem-dependent settings                                Line 34 of 352
Command ===> _____________________________________________ Scroll===> CSR_
                                                 12 Oct 1994 02:10
  Complex  System   SMF subsystems Audit concerns Priority
  SMFS@510 ML1E                9              5       29
  Pri Subs Su# Wr# Pa# Ex# Det Interval Recording activity summary
   29 RCT7 252   1   3   1 No  00:15:00 Write 100(5:8) 101(1,2,8:10) 102 103(64
 Exit     Address  Record  Act Record description
 IEFACTRT 00E795C8 29      No
                   30      No  Common Address Space Work
                   30-1    No  Job start
                   30-2    No  Interval
                   30-3    No  Step termination
                   30-4    No  Step total
                   30-5    No  Job termination
                   30-6    No  System address space
                   31      No  TIOC Initialization
                   32      No  TSO/E User Work Accounting
                   32-1    No  TSO/E User Interval
                   32-2    No  TSO/E User Session End
                   32-3    No  TSO/E User Detail Interval Record
                   32-4    No  TSO/E User Detail Session End
                   33      No  APPC/MVS TP Accounting
                   33-1    No  APPC/MVS Transaction
                   33-2    No  APPC/MVS Conversation
                   34      No  TS-Step Termination
```

Figure 331. SMF Subsystem Detail Display

The detail display contains the following fields of interest:

Table 225. SMF Subsystem Overview detail display - field descriptions

Field	Explanation
Exit	Name of an exit active for the subsystem.
Address	Address of the exit. (Is blank on MVS 5.1 and up.)
Record	Record number, in the format 'type-sub-type'. Each sub-type known, or referred to in SMFPRMxx, is shown separately.
Act	Indicates whether recording is active for this record type and sub-type.
Record description	A description of the record type and sub-type.

A sample batch report is shown in Figure 332 on page 450.

```
S M F   S U B S Y S T E M   O P T I O N S   12 Oct 1994 02:10
SMF subsystem-dependent settings


Complex  System   SMF subsystems Audit concerns Priority
SMFS@510 ML1E                  9              5       29

 Pri Subs Exit     Address  Det Interval Su# Wr# Pa#

  29 RCT4 IEFACTRT          No  00:15:00 253   1   2
      Recording activity: Write 100(5:8) 101(1,2,8:10) 102
      Audit concern:      RACF records suppressed, Job start not recorded, Datas
  29 RCT5 IEFACTRT          No  00:15:00 254   2   0
      Recording activity: Write 32 40
      Audit concern:      RACF records suppressed, Job start not recorded, Datas
  29 RCT6 IEFACTRT          No  00:15:00 252   2   2
      Recording activity: Write 100(5:8) 101(1,2,8:10) 102:103
      Audit concern:      RACF records suppressed, Job start not recorded, Datas
  29 RCT7 IEFACTRT          No  00:15:00 252   1   3
      Recording activity: Write 100(5:8) 101(1,2,8:10) 102 103(64:127)
      Audit concern:      RACF records suppressed, Job start not recorded, Datas
   5 STC  IEFUSO            No  00:15:00  14 242   0
          IEFUJP
          IEFU85
          IEFU84
          IEFU83
          IEFU29
      Recording activity: Suppress 14:19 62:69
      Audit concern:      Dataset activity not recorded
     RCT1 IEFACTRT          No  00:15:00   1 253   2
      Recording activity: Suppress 100(5:8) 101(1,2,8:10) 102
      Audit concern:
     RCT2 IEFACTRT          No  00:15:00   2 254   0
      Recording activity: Suppress 32 40
      Audit concern:
     RCT3 IEFACTRT          No  00:15:00   2 254   0
      Recording activity: Suppress 32 40
      Audit concern:
     SYS  IEFUAV            Yes 00:15:00   0 256   0
          IEFU29
          IEFUTL
          IEFUJI
          IEFUSO
          IEFUJP
          IEFUSI
          IEFUJV
          IEFACTRT
          IEFU85
          IEFU84
          IEFU83
      Recording activity: Write 0:255
      Audit concern:
```

Figure 332. Batch SMF Subsystem Report

SUBSYS - Subsystem report

The subsystem report describes the MVS subsystems, their communications tables, and their function tables. The most common security exposures are recognized, and the subsystems receive a relative audit priority accordingly.

This report requires a `CKFREEZE` file. A non-authorized zSecure Collect run suffices.

Background

A subsystem is a program, or set of programs, that performs a set of functions, either on behalf of MVS, or whenever MVS requests the subsystems to perform a

specific function. An example (and required) subsystem is JES; other subsystems are NetView® and IMS. Subsystems are heavily used by third-party products as well as IBM products.

MVS communicates with the subsystems through the subsystem interface (SSI) Each subsystem has a subsystem control block (SSCT), which declares its presence and its name. In addition, each subsystem can have a communication vector table (SSVT), which contains a list of functions, indexed by number. MVS requests subsystem actions by this function number and depending on the function type, it goes to all subsystems (a *broadcast* function); to a specific subsystem; or to all subsystems in turn, until a subsystem handles the request. Each SSCT also has two 'user fields', SUSE and SUS2, which can be used to store numbers or pointers. Figure 333 shows an overview of the SSCT and SSVT subsystem structure.

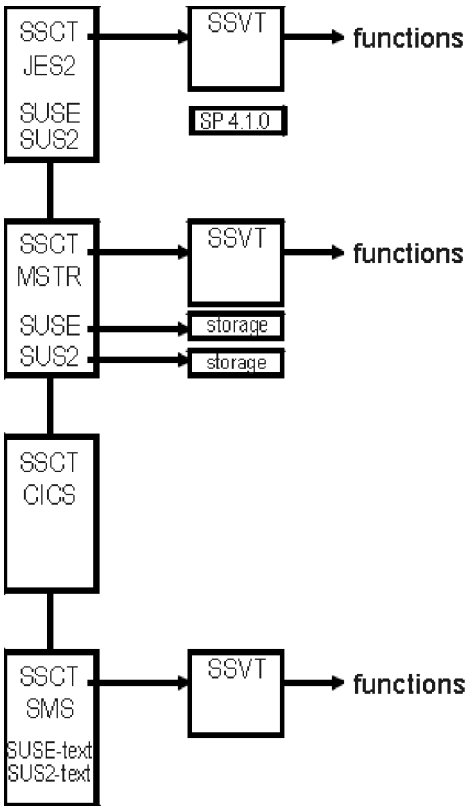


Figure 333. Subsystem Control Blocks

Subsystems are being used for the following purposes:

1. Intercepting MVS events like operator commands, WTO(R) messages, task termination, and address space termination. These are broadcasted to all subsystems (SSVT functions 4, 8, 9 ,10, and 50). Examples: JES, RACF.
2. Provide a system-wide calling interface to routines residing in common storage. The caller only specifies a function code. Example: SMS.
3. Provide a globally accessible storage anchor for subsystem control blocks. The SSCT contains two 'user' fields, SUSE and SUS2. The SSVT is not required for this purpose. An IMS subsystem is an example.

4. Provide a task (TCB) specific storage anchor for a subsystem. The Subsystem Affinity Table (SSAT) provides a fullword for each subsystem. No SUSE, SUS2, and SSVT pointers are required. This looks the same as a currently unused SSCT.

Auditing subsystems

The following considerations apply when auditing subsystems:

- Looking at the subsystem tables indicates which subsystem types a site has defined, and whether multiple versions are running at the same time.
- The order of the subsystems influences who gets control first for broadcast requests like operator commands and WTO(R).
- If a subsystem initialization has obtained its storage in a user storage key, programs from any address space can modify the control blocks of the subsystem. For instance, if the SSVT is in key 8, a broadcast function might be redirected causing the subsystem to remain uninformed or causing malicious code to get control. Similarly, the SSCT and areas pointed to by the user-pointers SUSE and SUS2 must not be writable.
- All information shown is available to unauthorized programs.

The batch report to review the subsystems is CKALSSCT. The interactive reports are called CKADSSC0 (concise) and CKADSSCT (detailed).

Note: The following displays first show the concise version of the subsystem report, and then describe the detailed report.

The concise subsystem overview display is shown in Figure 334.

```
Subsystem Communication Vector (concise)                        Line 1 of 16
Command ===> _____________________________________________ Scroll===> CSR
                                              11 Sep 2006 00:07
   Complex  System   Count Audit concerns Priority
   DINO     DINO        16              0
   Pri Name Org Type SUSE dat SUS2 dat Description
__     JES2   1 JES2 z/OS 1.4 ........ IBM JES2 Job Entry System
__     MSTR   2                        IBM MVS Master Scheduler
__     RACF   3      RSVT1..4          IBM RACF Resource Access Facility
__     OAM1   4                        IBM DFSMS Object Access Method
__     DFRM   5      ........ ........ IBM DFSMS removable media manager
__     CICS   6      ........          IBM CICS/Transaction Server
__     CNMP   7      NETV.... ........ IBM Netview (network management)
__     FFST   8                        IBM First Failure Support Technology pro
__     IRLM   9                        IBM IMS/VS Resource Lock Mgr
__     JRLM  10                        IBM IMS/VS Resource Lock Mgr
s_     SMS   11                        IBM DFSMS Storage Management System
__     LOGR  12                        IBM System Logger
__     RRS   13                        IBM Resource Recovery Services
__     SVAA  14      ........ NIT .. 1
__     TNF   15      TNF_CVT  ........ IBM TCP/IP (network facility)
__     VMCF  16      VMCF_CVT ........ IBM TCP/IP (network facility)
****************************** Bottom of Data ********************************
```

Figure 334. Subsystem overview display (concise)

The overview panel contains the following fields of interest.

Table 226. Subsystem Communication Vector (concise) display - field descriptions

Field	Explanation
Complex	The name of the complex
System	The name of the system.

Table 226. Subsystem Communication Vector (concise) display - field descriptions (continued)

Field	Explanation
Count	The number of subsystems defined.
Audit concerns	The number of subsystems with audit concerns.
Priority	The highest audit priority found.
Pri	The audit priority of the subsystem.
Name	The subsystem name.
Org	The position of the subsystem in the subsystem chain.
Type	JES subsystem type: JES2, JES3, or blank.
SUSE dat	The first eight characters from the SUSE contents.
SUS2 dat	The first eight characters from the SUS2 contents.
Description	Name of the package normally creating this subsystem.
Audit concern	Audit concerns identified.

Select any subsystem for a detail display.

```
Subsystem Communication Vector (concise)                        Line 1 of 8
Command ===> _____________________________________________ Scroll===> CSR
                                                  11 Sep 2006 00:07
   Complex  System   Count Audit concerns Priority
   DINO     DINO        16              0
   Pri Name Org Type SUSE dat SUS2 dat Description
       SMS   11                        IBM DFSMS Storage Management System

Function Description                          Where   Entry at
       8 End-of-Address Space                 EPLPA   IGDZILLA
      15 Verify Subsystem                     EPLPA   IGDZILLA
      16 Open Data Set                        EPLPA   IGGS0OPN
      17 Close Data Set                       EPLPA   IGGS0CLS in IGGS0OPN
      55 SMS Exit/Services                    EPLPA   IGDZILLA

****************************** Bottom of Data ********************************
```

Figure 335. Subsystem detail display (concise)

The detail display contains the following fields of interest.

Table 227. Subsystem Communication Vector (concise) detail display - field descriptions

Field	Explanation
Function	Function code supported by subsystem.
Description	The description of the subsystem function.
Where	Function residency.
Entry at	Module and offset information for the subsystem function.

The next set of displays shows the detailed subsystem report. You are advised to skip these displays, and use concise reporting, until you are familiar with the subsystem report. For clarity, the same system and subsystem is examined as in the concise displays above.

The detailed overview display shows an overview of the subsystems defined, sorted first in order of relative audit priority, then by original order.

```
Subsystem Communication Vector Tables                          Line 1 of 16
Command ===> _____________________________________________ Scroll===> CSR
                                                  11 Sep 2006 00:07
   Complex  System   Count Audit concerns Priority
   DINO     DINO        16              0
   Pri Name Org Type MFn FIB PSS ARD SUSE dat SUS2 dat Description
__     JES2   1 JES2  28 Yes No  Yes z/OS 1.4 ........ IBM JES2 Job Entry Syste
__     MSTR   2        6 No  No  No                     IBM MVS Master Scheduler
__     RACF   3      256 No  Yes No  RSVT1..4           IBM RACF Resource Access
__     OAM1   4        0 No  Yes No                     IBM DFSMS Object Access
__     DFRM   5      256 No  No  No  ........ ........ IBM DFSMS removable medi
__     CICS   6        4 No  Yes No  ........           IBM CICS/Transaction Ser
__     CNMP   7        5 No  No  No  NETV.... ........ IBM Netview (network man
__     FFST   8        0 No  No  No                     IBM First Failure Suppor
__     IRLM   9        0 No  No  No                     IBM IMS/VS Resource Lock
__     JRLM  10        0 No  No  No                     IBM IMS/VS Resource Lock
s_     SMS   11        3 No  No  No                     IBM DFSMS Storage Manage
__     LOGR  12        5 No  No  No                     IBM System Logger
__     RRS   13        0 No  No  No                     IBM Resource Recovery Se
__     SVAA  14        2 No  Yes No  ........ NIT .. 1
__     TNF   15        0 No  No  No  TNF_CVT  ........ IBM TCP/IP (network faci
__     VMCF  16        0 No  No  No  VMCF_CVT ........ IBM TCP/IP (network faci
****************************** Bottom of Data ********************************
```

Figure 336. Subsystem overview display

The overview panel contains the following fields of interest.

Table 228. Subsystem Communication Vector Tables - field descriptions

Field	Explanation
Complex	The name of the complex.
System	The name of the system.
Count	The number of subsystems defined.
Audit concerns	The number of subsystems with audit concerns.
Priority	The highest audit priority found.
Pri	The audit priority of the subsystem.
Name	The subsystem name.
Org	The position of the subsystem in the subsystem chain.
Type	JES subsystem type: JES2, JES3, or blank.
MFn	The maximum number of function entry points that can be defined. Each entry point can be used for several function codes.
FIB	Indicates whether serialization of Forward-In-Background (FIB) requests is required. E.g. TSO provides the FIB commands SUBMIT, CANCEL, and START.
PSS	Indicates whether the subsystem requires Primary Subsystem Support (PSS). If set, the subsystem is started under the primary JES. If not set, it is started under the master (MSTR) subsystem.
ARD	Indicates whether the subsystem supports the allocation of a special internal reader.
SUSE dat	The first eight characters from the SUSE contents.
SUS2 dat	The first eight characters from the SUS2 contents.
Description	Name of the package normally creating this subsystem.
Audit concern	Audit concerns identified.

Select any subsystem for a detail display. Within the detail display, you can scroll right to see more information on the subsystem functions.

```
Subsystem Communication Vector Tables                          Line 1 of 13
Command ===> _____________________________________________ Scroll===> CSR
                                                  11 Sep 2006 00:07
   Complex  System   Count Audit concerns Priority
   DINO     DINO        16              0
   Pri Name Org Type MFn FIB PSS ARD SUSE dat SUS2 dat Description
       SMS   11        3 No  No  No                    IBM DFSMS Storage Manage

Pointer  Address  Where   Key  SP          Eye catcher
SSCT     00C0D610 CSA       0 241
SSCTSUSE 00000000
SSCTSUS2 00000000
SSCTSSVT 00C1B508 CSA       0 241
Function Address  Where   Key  SP Program  Description
       8 04CC94E8 EPLPA           IGDZILLA End-of-Address Space
      15 04CC94E8 EPLPA           IGDZILLA Verify Subsystem
      16 04E5A1F8 EPLPA           IGGS0OPN Open Data Set
      17 04E62CB0 EPLPA           IGGS0CLS Close Data Set
      55 04CC94E8 EPLPA           IGDZILLA SMS Exit/Services

****************************** Bottom of Data ********************************
```

Figure 337. Subsystem detail display

The detail display contains the following fields of interest.

Table 229. Subsystem Communication Vector Tables - additional field descriptions

Field	Explanation
SSCT	Location, residence, key, and subpool of the SSCT.
SSCTSUSE	Location, residence, key, subpool, and first 8 bytes of the SSCT SUSE user pointer.
SSCTSUS2	Location, residence, key, subpool, and first 8 bytes of the SSCT SUS2 user pointer.
SSCTSSVT	Location, residence, key, and subpool of the SSCT SSVT pointer.
Function	Function code supported by subsystem.
Address	Function entry point.
Where	Function residency.
Key SP	Key and subpool of the memory area where the function resides.
Program	Module name of the subsystem function.
Description	A description of the subsystem function.
InstrSc	Results from an instruction scan on the subsystem function.
Str	Results from a string scan on the subsystem function.
Length	Approximate length of the subsystem function.
AM	Addressing mode
Entry at	Module and offset information for the subsystem function.
Eye catchers	Storage display of the subsystem function.

VSM/WRITABLE - Memory reports

Security zSecure provides reports on the virtual memory layout of the system and the structure of the common storage. These report types can be generated for a live MVS system or using a CKFREEZE file.

This report is available on a live system. Consequently, no CKFREEZE file is required.

Background

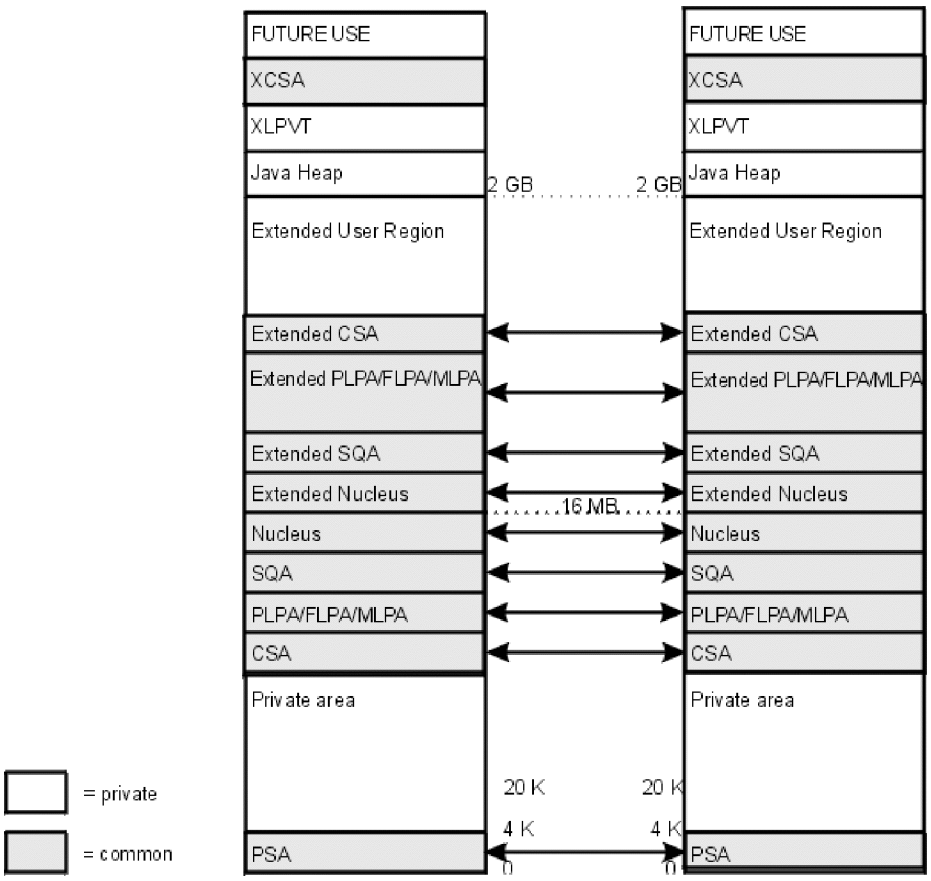


Figure 338. Virtual Memory Layout

Figure 338 shows the virtual memory layout of an MVS system. The location and size of each memory area is configuration-dependent. The shaded areas are *common* storage. Common storage areas are present and identical in every address user space. The non-shaded areas are *private*. Changes to private areas are local to one user. Changes to common storage are visible to and can affect every user and program on the system.

Security zSecure can report the storage areas location and size, which helps determine the residency of programs and tables known by address. In most Security zSecure reports, the memory areas are listed in the WHERE field. The data includes the percentage of CSA and ECSA used and the signals overflow into (E)SQA. The batch report for reviewing the system memory map is CKALSVSM. The interactive report is called CKADSVSM.

Auditing memory

Security zSecure can also report on the used memory areas in (E)CSA and (E)SQA. The report provides the location and size of each area as well as the storage protection key and subpool used. Shared memory areas with a storage protection key (*user key*) of 8 or higher might be a cause for concern. With this setting, any user might be able to change the memory which affects the operation of the program that uses the memory area. The sample reports to review common storage focus on these memory areas. If you want to report on not only the vulnerable, but all allocated common storage, you will need to edit the sample reports. The batch report to find writable common storage is CKALSCSM. The interactive report is CKADSCSM.

Sample ISPF displays are shown in the following figures. The batch reports are equivalent and are not included.

```
Virtual storage map                                              Line 1 of 21
Command ===> _____________________________________________ Scroll===> CSR
                                          21 Sep 2001 10:22
   Complex  System   Count Audit concerns Priority
   C#M4     C#M4        21              0
   Pri Type              Start address       End address          Area Length %
 __    XCSA          00000200_00000000 0001FFFF_FFFFFFFF      560750930165760
 __    XLPVT         00000008_00000000 000001FF_FFFFFFFF        2194728288256
 __    JAVA                  80000000 00000007_FFFFFFFF          32212254720
 _     EPVT                  0D700000          7FFFFFFF           1922039808
 _s    ECSA                  05E4C000          0D6FFFFF            126566400
 __    EMLPA                 05680000          05E4BFFF              8175616
 __    EFLPA                 0567D000          0567FFFF                12288
 __    EPLPA                 027B9000          0567CFFF              49037312
 __    ESQA                  01A5C000          027B8FFF              14012416
 __    ENUC RW               019F6000          01A5BFFF                417792
 __    ENUC RO slack         019F57D0          019F5FFF                  2096
 __    ENUC RO               01000000          019F57CF              10442704
 __    NUC RO                00FE4000          00FFFFFF                114688
 __    NUC RW slack          00FE3280          00FE3FFF                  3456
 __    NUC RW                00FD4000          00FE327F                 62080
 __    SQA                   00D61000          00FD3FFF               2568192
 __    PLPA                  00BAB000          00D60FFF               1794048
 __    FLPA                  00BAA000          00BAAFFF                  4096
 __    MLPA                  00B93000          00BA9FFF                 94208
 __    CSA                   00700000          00B92FFF               4796416
 __    PVT                   00001000          006FFFFF               7335936
 __    PSA                   00000000          00000FFF                  4096
 ****************************** Bottom of Data ********************************
```

Figure 339. Virtual Storage Map

```
Virtual storage map                                              Line 1 of 10
Command ===> _____________________________________________ Scroll===> CSR

                                          21 Sep 2010 10:22
Storage area type            ECSA

Start address                             05E4C000
End address                               0D6FFFFF
Length of storage area                    126566400
%Area in use                                    41%

Pri Audit concern

****************************** Bottom of Data ********************************
```

Figure 340. Virtual Storage Map details

The display in Figure 341 on page 458 shows writable common storage.

```
Globally Writable Common Storage
Command ===> _____________________________________________ Scroll===> CSR_
                                                 6 Jan 2004 06:14
   Complex  System   Count Audit concerns Priority
   ZETP     S0W1         2              2       25
Pri Type     Start address       End address          Area length Key SP  Aud
 25  CSA          00B6B000          00B6BFFF                4096   8 231 Mem
 25 XCSA 00000200_00000000 00000200_001FFFFF             2097152   8     Mem
****************************** Bottom of Data ********************************
```

Figure 341. Writable Common Storage Display

MPFMSG - MPF report

This report shows the message-specific data from the Message Processing Facility.

This report requires a CKFREEZE file. A non-authorized zSecure Collect run suffices.

Background

The MVS Message Processing Facility (MPF) allows the installation to alter the handling of system messages, which are normally displayed on operator consoles. Message handling is performed on the basis of the *message id*; in addition, a message handling default can be set, and is applied to all messages not handled explicitly. This default is shown as message id .NOENTRY.

MPF allows the message to be:

- Suppressed. If suppressed, it is not displayed on the operator consoles. It is included in the SYSLOG, unless the message has a routing code not included in SYSLOG.
- Automated. If automated, the message is made available to an automation subsystem, such as NetView.
- Sent to an exit. The exit is called each time the system issues the message, and is supposed to handle message processing. The exit can suppress the message.

The MPF parameters are specified in parmlib members MPFLSTxx. Several MPFLSTxx members can be active at the same time.

Auditing Message Processing

The following considerations apply when auditing MPF parameters:

- Check the messages that are suppressed. Sensitive messages, such as ICH408I on a RACF system, should not be suppressed if your installation has a security console.
- Check the exits used to process messages.
- Check the default handling of messages.
- Check the messages that are, and those that are not, automated.

The batch report to review MPF is CKALSMSG. The interactive report is called CKADSMSG.

Figure 342 on page 459 shows the MPF overview display.

```
Message Processing Facility message intercepts                  Line 1 of 142
Command ===> _____________________________________________ Scroll===> CSR_
                                                  25 Feb 1998 00:05
   Complex  System   Count Suppress Automate ExitCall Audit concerns Priority
   C#M4     C#M4       142      130        7       10            137       20
   Pri Msg id     Sup Auto     Member   Exit     Address  Where   Exit at
__  20 ICH70001I  YES NO       MPFLST00
__  20 IRR806I    YES NO       MPFLST00
s_   1 $HASP001   YES NO       MPFLST00
__   1 $HASP002   YES NO       MPFLST00
__   1 $HASP100   YES NO       MPFLST00
__   1 $HASP110   YES NO       MPFLST00
__   1 $HASP111   YES NO       MPFLST00
__   1 $HASP112   YES NO       MPFLST00
__   1 $HASP113   YES NO       MPFLST00
```

Figure 342. Message Processing overview display

The display contains the following fields of interest:

Table 230. Message Processing Facility message intercepts - field descriptions

Field	Explanation
Complex	The complex name.
System	The system name.
Count	The number of message ids processed by MPF.
Suppress	The number of message ids suppressed by MPF.
Automate	The number of message ids automated by MPF.
ExitCall	The number of message ids for which an exit is called.
Audit concerns	The number of message ids for which audit concerns were identified.
Priority	The highest audit priority identified.
Pri	The current entry's audit priority.
Msg id	The message id of one message. All fields on the rest of the line apply to that message id.
Sup	Indicates whether the message is suppressed.
Auto	Indicates whether the message is automated; if it is, it contains the automation token.
Member	The parmlib member from which the MPF definition was taken.
Exit	The name of the exit called for the message.
Address	The address of the exit.
Where	Residency of the exit.
Exit at	Module information on the exit.
Audit concern	Audit concerns identified.

Figure 343 on page 460 shows the MPF detail display. It does not show additional information.

```
Message Processing Facility message intercepts                  Line 1 of 12
Command ===> ____________________________________________ Scroll===> CSR_
                                          25 Feb 1998 00:05
   Complex  System   Count Suppress Automate ExitCall Audit concerns Priority
   C#M4     C#M4       142      130        7       10            137       20
   Pri Msg id     Sup Auto     Member   Exit     Address  Where   Exit at
     1 $HASP001   YES NO       MPFLST00

Message id                    $HASP001
Suppress message              Yes
Automation for messages       NO
Parmlib member                MPFLST00
Exit name
Exit address
Exit residency
Exit load module information

Audit concern
Message suppressed
****************************** Bottom of Data ********************************
```

Figure 343. Message Processing detail display

JOBCLASS - JES2 Job Class report

The JES2 job class report can be used to review the protection of the JES2 job classes for each system.

This report requires a CKFREEZE file made in an APF-authorized run of zSecure Collect.

Background

The JES2 job class definitions specify the attributes of each job class, such as default region size and time limits, command authorization, and SMF logging. The job class is usually selected through the CLASS= parameter in the JCL, but some sites assign a job class through an exit (IEFUJV, or JES2 exit 2 or 6).

The following security considerations apply to JES2 job class definitions:

- Users can issue MVS commands embedded in JCL. For each job class, an *authority level* determines the type of commands that can be issued, and a *command disposition* determines whether the command is ignored, must be verified by an operator, or is executed without verification. (The command authority level is determined through SAF, using resource names in the OPERCMDS class.)
- Bypass Label Processing (BLP) can be requested through the LABEL parameter of JCL DD command. If BLP is not allowed, all BLP requests are converted to NL (Non-Labelled).

  If BLP is allowed, users might be able to circumvent the protection of tape data sets. A job with BLP is allowed to ignore the actual data set name and volume serial on a tape JES2 leaves the JCL as it is, and leaves the authorization to a security product. DFP does a SAF request on the resource ICHBLP in the class FACILITY; READ access is required if the data set is opened for input, and UPDATE access is required for output.

  RACF can be used to control BLP. This requires both the TAPEVOL and FACILITY classes to be active; RACF checks the access of the user on the ICHBLP resource name in the FACILITY class.
- The writing of SMF record types 6 and 26 (JES2 output writer and Job Purge records) can be determined on a per-job-class basis. (If JES2 does attempt to

write these records, they can still be suppressed on a per-subsystem basis; see "SMFSUBOP - SMF subsystem report" on page 446.)

- The use of the JES2 exits IEFUJP (job purge exit) and IEFUSO (SYSOUT limit exit) can be determined on a per-job-class basis. If these exits are used in your installation, check that all active job classes use these exits.

Auditing Job Classes

The following considerations apply when auditing JES2 job classes:

- Check the command authorization and disposition. Check whether the OPERCMDS class is active, and check the profiles defined in the OPERCMDS class.class. Security zSecure warns you if the class is not active, or if the default return code of the class is too low.
- Check whether the job class allows BLP. If the job class allows BLP, check whether RACF is used to control it. Security zSecure warns you if the appropriate classes are not active, if no profile has been defined, or if the UACC on the profile used is READ or higher.
- If your installation requires SMF record types 6 and 26 to be written, check whether the job classes do not suppress these record types.
- Check whether the use of the IEFUJP and IEFUSO exits matches the requirements of your installation.
- Check whether the job class requirements for account numbers match the requirements of your installation.

The batch report to review the JES2 job classes is CKALSJCL. The interactive reports are called CKADSJC0 (concise) and CKADSJCL (detailed).

Note: The following figures show the detailed version of the job class report. The concise version of the report contains less information.

Sample ISPF overview and detail displays for the job class report are shown in the following figures.

```
JES2 Job Class parameters (e.g. MVS command auth / BLP)          Line 1 of 36
Command ===> _____________________________________________ Scroll===> CSR_
                                                 6 Dec 1994 09:13
   Complex  System   Subsys Classes Audit concerns Priority
   IPO1     IPO1      JES2       36             13       45
   Pri C Command Auth commands    BLP HOLD ACCT Time      Regio SWA   PL UJP US
s_  45 O EXECUTE ALL              Yes No   Yes  000060,00 0005M BELOW 00 Yes Ye
__  26 1 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 2 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 01 Yes Ye
__  26 3 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 01 Yes Ye
__  26 4 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 5 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 6 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 7 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 8 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  26 9 VERIFY  ALL               No  No   No   000030,00 0001M BELOW 00 Yes Ye
__  25 M VERIFY  ALL               No  No   Yes  000060,00 0005M BELOW 00 Yes Ye
__  25 N VERIFY  ALL               No  No   Yes  000060,00 0005M BELOW 00 Yes Ye
__  20 P VERIFY               INFO Yes No   Yes  000060,00 0005M BELOW 00 Yes Ye
__     A IGNORE  ALL               No  No   Yes  000060,00 0005M BELOW 00 Yes Ye
__     B IGNORE  ALL               No  No   Yes  000060,00 0005M BELOW 00 Yes Ye
__
```

Figure 344. Job class overview display

The overview display lists the job classes defined, sorted by audit priority. Job class O is considered a serious security problem, as indicated by an audit concern above 40.

Job class O is selected to show a detail display.

```
JES2 Job Class parameters (e.g. MVS command auth / BLP)          Line 1 of 36
Command ===> ____________________________________________________ Scroll===> CSR_
                                                  6 Dec 1994 09:13
   Complex  System   Subsys Classes Audit concerns Priority
   IPO1     IPO1     JES2        36             13       45
   Pri C Command Auth commands    BLP HOLD ACCT Time      Regio SWA   PL UJP US
    45 O EXECUTE ALL              Yes No   Yes  000060,00 0005M BELOW 00 Yes Ye

Command disposition           EXECUTE
Authorized command groups     ALL
Bypass Label Processing       Yes
Jobs held until released      No
Account number required       Yes
Time limit                    000060,00
Region size                   0005M
SWA control block residency   BELOW
PROCxx suffix         PROCLIB 00
Job purge exit IEFUJP taken   Yes
SYSOUT limit exit IEFUSO take Yes
SMF Type 6 record written     Yes
SMF Type 26 record written    Yes

Audit concern
BLP RACF-protected, MVS Modify commands allowed, low RC on OPERCMDS, not
verified by operator
******************************* Bottom of Data ********************************
```

Figure 345. Job Class Detail Display

The audit concern for the job class makes the problem clear: MVS modify commands are allowed, not protected by RACF, and not verified by the operator. This allows any user to embed MVS commands in JCL, and then have them executed. BLP is allowed, but RACF-protected, so this is not a problem.

The displays contains the following fields of interest:

Table 231. Job Class Detail Display - field descriptions

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Subsys	The name of the JES2 subsystem.
Classes	The number of classes defined in the subsystem.
Audit concerns	The number of classes for which audit concerns were identified.
Priority	The highest audit priority identified.
Pri	Numerical audit priority.
C	The name of the job class.
Command	Indicates the command disposition, that is, the action taken by JES2 for MVS commands received. Can be any of the following: VERIFY (verify by operator) DISPLAY (display and execute) EXECUTE (execute but do not display) IGNORE (ignore silently)

Table 231. Job Class Detail Display - field descriptions (continued)

Field	Explanation
Auth commands	The command type authorized for the job class. Can be ALL (all command types) SYS (system commands) CONS (console commands) IO (input/output commands) and INFO (information commands)
BLP	Indicates whether Bypass Label Processing (BLP) is allowed.
HOLD	Indicates whether jobs are held before starting (these must be released by the operator). Some sites only allow BLP in combination with HOLD (as a security measure).
ACCT	Indicates whether account information is required.
Time	Indicates the default time limit.
Regio	Indicates the default region size.
SWA	Indicates SWA control block residency: above or below the 16 MB line virtual storage.
PL	Indicates the PROCLIB suffix
UJP	Indicates whether the IEFUJP job purge exit is taken.
USO	Indicates whether the IEFUSO SYSOUT limit exit is taken.
T6	Indicates whether SMF 6 records are written.
T26	Indicates whether SMF 26 records are written.
Audit concern	Audit concerns identified.

CONSOLE - Console report

The console report describes the system consoles for each system. Additional system-wide console parameters are displayed in the MVS settings report (“SYSTEM - MVS system settings report” on page 441).

This report requires a CKFREEZE file. A non-authorized zSecure Collect run is sufficient.

Background

MVS uses *operator consoles* as the principal means of communicating with the system. If all other I/O fails, MVS can still communicate through the hardware or system console. In addition to the system console, typically a number of MCS (Multiple Console Support) consoles are defined. MCS consoles are devices that are locally attached. In addition, consoles can be defined on devices accessed through z/OS Communications Server; these are called SMCS consoles. Also, software applications like TSO and SDSF can define *virtual* consoles called EMCS.(Extended MCS) consoles. There is also an older software method to create *subsystem consoles*, but their use is diminishing.

Each console can be limited with respect to the commands that can be entered on the console, through the AUTHORITY attribute. The least powerful authority is INFO. Increasingly powerful are CONS, IO, SYS and MASTER. If a console has MASTER authority, it can execute any MVS command. The only way to curb

MASTER authority is to use SAF controls - requiring LOGON for authentication and authorizing the actual command through the OPERCMDS class, based on the user identity, on the actual console being used or both.

The console parameters are specified in parmlib member CONSOLxx. For more information see the manual "MVS Operations: planning". For the current CONSOLxx member suffix, see “IPLPARM - IPL parameters report” on page 444.

Note that EMCS consoles are only shown on the report if a CKFREEZE data set is used that has been made with zSecure Collect 1.5.0 or higher running APF authorized.

Auditing Consoles

The following considerations apply when auditing consoles:

- Review the consoles defined, and the messages routed to each console. If a console has been defined for a specific purpose for example, as a security console, make sure the routing codes and message level have been set correctly.
- Check whether a logon is required for the consoles. This is a system-wide parameter that is set for all or none of the consoles. If any system console resides in a physically insecure area, the logon requirement should be set to REQUIRED. For a B1 system, the logon requirement should always be set to REQUIRED, except for the hardware console.
- Check the command authority for the consoles. The consoles that allow all command types to be issued should reside in a physically secure area. While Security zSecure cannot verify the location of any console, the device number can be used to track down the console.
- SMCS consoles without predefined LU are especially dangerous, since they can be accessed from anywhere. When login is optional and they fall under a catchall CONSOLE profile or the class is inactive, they can be accessed by anybody, and only class OPERCMDS safeguards which operator commands can be issued. When login is automatic, it also warrants inspection.
- For z/OS releases prior to z/OS 1.8, check whether an alternate console has been defined for essential consoles.

The batch report to review the consoles is CKALSCON. The interactive report is called CKADSCON.

Sample ISPF overview and detail displays for the console report are shown in the following figures.

```
Operator Consoles                                                Line 1 of 41
Command ===> _____________________________________________ Scroll===> CSR_
                                          7 Apr 2005 00:07
   Complex  System   Consoles Audit concerns Priority
   DINO     DINO          41              2       20
   Pri Type      Name     Act Con Log Userid   Jobname  LUname   Devn Authority
__  20 MCS       01       No    1 Opt                             900 ALL
__  20 MCS       02       No    2 Opt                             901 ALL
__     EMCS      AUTO1NM  Yes                CNMPROC  AUTO1          MASTER
__     EMCS      BERTTICB No                         IPDINO30       MASTER
__     EMCS      C#TELNET No                         C#TELNET
__     EMCS      CATO#EXP No                         C##BERTC
__     EMCS      CNMCRNM  Yes                CNMPROC  CNMCSSIR
__     EMCS      C##AINT  No                         IPDINO14       MASTER
__     EMCS      C##BDV25 No                         IPDINO06
__     EMCS      C##BERT  No                         IPDINO28       MASTER
__     EMCS      C##BERT1 No                         IPDINO22
__     EMCS      C##BERT2 No                         IPDINO03
__     EMCS      C##BERT5 No                         IPDINO14
__     EMCS      C##BERT8 No                         IPDINO14
__     EMCS      C##BFT1  No                         IPDINO24       MASTER
__     EMCS      C##BGUS  No                         IPDINO12       MASTER
__     EMCS      C##BHJ1  No                         IPDINO21       MASTER
__     EMCS      C##BHJ12 No                         IPDINO23
__     EMCS      C##BJTI1 No                         IPDINO26
__     EMCS      C##BLU11 No                         IPDINO20
__     EMCS      C##BMR1C No                         IPDINO23       MASTER
__     EMCS      C##BMR11 No                         IPDINO28
__     EMCS      C##BMR12 No                         IPDINO23
__     EMCS      C##BMR13 No                         IPDINO28
__     EMCS      C##BMR21 No                         IPDINO18
__     EMCS      C2PWTOXX Yes                C2POLICE C2PWTOXX      MASTER
__     EMCS      DEVLST30 No                         COMMANDR
__     EMCS      DINO     Yes 100                    DINO           MASTER
__     EMCS      R##SLIN2 No                         IPDINO04
__     EMCS      R##SLIN3 No                         IPDINO15
__     EMCS      R##SLIN4 No                         IPDINO15
__     SubSystem 03       No    3                                  ALL
__     SubSystem 04       No    4                                  ALL
__     SubSystem 05       No    5                                  ALL
__     SubSystem 06       No    6                                  ALL
__     SubSystem 07       No    7                                  ALL
__     SubSystem 08       No    8                                  ALL
```

Figure 346. Console Report

The display contains the following fields of interest:

Table 232. Console report - field descriptions

Field	Explanation
Complex	Name of the complex described
System	Name of the system described.
Consoles	Number of system consoles defined.
Audit concerns	Number of system consoles for which audit concerns were identified.
Priority	The highest audit priority found for any console.
Pri	The audit priority for the console.
Type	The type of the console; either MCS, EMCS, SubSystem, or blank if no console is connected.
Name	Name of the console.
Act	Whether the console is active or not. For subsystem consoles this is Yes when the console is dedicated to a subsystem, and No if it is in allocatable status.

Table 232. Console report - field descriptions (continued)

Field	Explanation
Con	The console number, counted per system. For EMCS consoles this field is empty.
Log	The system-wide logon requirement; can be OPT (optional), AUT (automatic), or REQ (required).
Userid	The `userid` logged on to the console.
Jobname	For in-use subsystem consoles, this is the subsystem to which the console is dedicated. For EMCS consoles this field contains the jobname that has the console activated.
LUname	The VTAM® Logical Unit name for SMCS consoles or terminal name for EMCS consoles.
Devn	The device number of the console.
Authority	The authority of the console. The master console has MASTER; the other consoles can have ALL (almost equal to master), or one or more from SYS (system commands), IO (I/O commands), CONS (console commands), and INFO (display commands).
CmdSys	System that receives the commands typed on the console. "*" means the system where the console is defined.
Profile	The name of the profile that protects the console.
Routecode	The routing codes of the console.
Level	The message level of the console. See “LEVEL” on page 1007 for a list of values.
Mon	Monitored events like JOBNAMES, SESSION, and STATUS.
HC	For EMCS consoles, this field indicates whether the console receives hardcopy-only messages.
Aut	For EMCS consoles, this field indicates whether the console receives messages that were automated by MPF.
UD	Indicates whether the console receives undirected messages.
Int	Receive messages for internal ids (console 0).
Unk	Receive messages for unknown console ids.
DOM	Whether this console receives Delete Operator Messages (DOM) and from where. It's values can be ALL (all systems in sysplex), NORMAL (this system), and NONE (no system).
Alternat	The name of the alternate console.
Jobid	For EMCS consoles this field contains the job id of the job that has the console activated.
PfkTab	The name of the function-key table used.
Switchto	The name of a console to which this console has been switched. Normally, this is empty.
Mig	Migration id of an EMCS console.
CNID	The CoNsole ID. Used to route commands, responses and messages.
Key	The key that is assigned by the OPERPARM data to an EMCS console.
Audit concerns	Audit concerns identified.

The console detail display is shown in Figure 347 on page 467.

```
Operator Consoles                                          Line 1 of 44
Command ===> _____________________________________________ Scroll===> CSR_
                                          7 Apr 2005 00:07

  Console identification
_ Complex name                  DINO
_ System name                   DINO
  Console name                  01
  Console type                  MCS
  Site-specified key
  Console number                1
  Migration console id
  Console id (CNID)             00000001

  Console user
  Console is active             No
  User logged on to console
  Job or subsystem name
  Jobid using EMCS console
  SMCS LU or EMCS termname

  Console authorization
  Command authority             ALL
_ System to send commands to    DINO

  Console protection
  Console logon                 Optional
  RACF profile in class CONSOLE **
  Alternate console name/group  02
  Switched to console
  Relative audit priority       20

  Console information shown
  Routing codes                 1:128
  Message level                 R I CE E IN NB
  Undirected messages           Yes
  Internal messages
  Unknown console id messages
  Receive hardcopy messages
  Receive msgs automated by MPF
  Events to be monitored        JOBNAMES
  Delete operator messages type

  Console properties
  Device number                  900
  Parmlib PFKTAB entry          PFKTAB1

  Audit concern
  System authority and no logon required
****************************** Bottom of Data ******************************
```

Figure 347. Console detail display.

The detail display does not contain any additional fields.

PPT - Program Property Table report

The Program Property Table report describes the MVS PPT, which defines special attributes for selected authorized programs.

The report requires a CKFREEZE file made in an APF-authorized run of zSecure Collect.

Background

The Program Property Table (PPT) is an MVS table that describes APF-authorized programs. It contains attributes that are assigned to these programs as they are loaded from an APF library as a job step program. These attributes can be taken from the default load module IEFSDPPT or from parmlib member SCHEDxx. For a

number of address spaces default PPT definitions are shipped with the operation system, and sometimes sites modify these.

The attributes that can be set in the PPT include the following:

- Bypass SAF. If the BYPASS flag is set, data set accesses by the program are not subject to SAF security checks.
- The key in which the job step runs. Keys in the range 0 to 7 imply authorization.
- Data set integrity. If the NODSI flag is set, data sets used by the program can be deleted by another program while still being used.

Auditing the Program Property Table

The following considerations apply when auditing the Program Property Table:

- A task that bypasses password and SAF protection is very dangerous if it can be called by arbitrary users and be induced to read from or write to user-specified data sets. So programs like HASJES20 and DFHSIP should never have bypass password authority, especially if there is no program protection in place. On RACF systems, you can use the Authorized Programs report in "APFPROT - Authorized Programs reports" on page 328 to check on the protection of PPT-authorized modules.
- Tasks with system key should be audited like AC(1) modules: they are authorized to bypass system security, and if you do not know anything about them you had better protect them from execution by arbitrary users.
- Tasks without data set integrity that depend on data sets can be brought down by accident (e.g. deleting/renaming a PROCLIB in JES2 can be done if HASJES20 has NODSI, but the next job conversion for the DDname causes JES2 to abend). So NODSI usually creates an availability risk.

The batch report to review the sensitive data sets is CKALSPPT. The interactive report is called CKADSPPT.

Sample ISPF overview and detail displays for the PPT report are shown in the following figures.

```
Program Property Table                                          Line 1 of 55
Command ===> ____________________________________________ Scroll===> CSR_
                                              26 Aug 1997 00:05
   Complex  System   Count Audit Concerns Priority
   C#M4     C#M4        55            54        8
   Pri Program  Key Bypass NoDSI Modif NonSwap NonCan Priv Systask Audit concer
__   8 HASJES2A   1        NoDSI Modif NonSwap NonCan Priv Systask Executes in
__   6 FNMMAIN    6              Modif NonSwap NonCan              Executes in
__   6 ICUMKG10   1              Modif                             Executes in
__   6 ICUMKM11   1              Modif                 Priv Systask Executes in
__   3 COFMINIT   0 Bypass NoDSI       NonSwap              Systask Bypasses SAF
s_   3 COFMISDO   0 Bypass NoDSI       NonSwap NonCan       Systask Bypasses SAF
__   3 IEEMB860   0 Bypass NoDSI       NonSwap NonCan       Systask Bypasses SAF
__   2 AKPCSIEP   1        NoDSI       NonSwap              Systask Executes in
__   2 APSPPIEP   1        NoDSI       NonSwap              Systask Executes in
__   2 CSVLLCRE   0 Bypass             NonSwap              Systask Bypasses SAF
__   2 ERBMFMFC            NoDSI Modif NonSwap              Systask No dataset i
__   2 ERB3GMFC            NoDSI Modif NonSwap              Systask No dataset i
__   2 HASJES20   1        NoDSI       NonSwap NonCan       Systask Executes in
__   2 IATINTK    1        NoDSI       NonSwap NonCan       Systask Executes in
__
```

Figure 348. Program Property Table overview display

The overview display contains the following fields of interest:

Table 233. Program Property Table overview - field descriptions

Field	Explanation
Complex	The name of the complex examined
System	The name of the system examined
Count	The number of PPT entries
Audit concerns	The number of PPT entries for which audit concerns were identified.
Priority	The highest audit priority found for any PPT entry.
Pri	The audit priority for the PPT entry.
Program	Name of the program.
Key	The PSW key in which the program runs. A key in the range 0 to 7 indicates authorization.
Bypass	Indicates whether the program bypasses SAF.
NoDSI	Indicates whether the program uses data set integrity (blanks) or not (NoDSI).
Modif	Indicates whether the entry has been modified (Modif) after the original initialization from the IEFSDPPT module (which supplies the defaults). If it was added to the table, it is considered modified too.
NonSwap	Indicates whether the program is marked non-swappable.
NonCan	Indicates whether the program can be cancelled (blank) or not (NonCan).
Priv	Indicates whether the program is privileged. A privileged program is not swapped unless in a long wait state.
Systask	Indicates whether the program is a system task (Systask) or not (blanks). A system task is not timed.
Audit concern	Audit concerns identified.

Note that some audit concerns might be suffixed with *(IBM default)*, which indicates that the program property is in the IBM supplied IEFSDPPT for the OS level being investigated. This indication is separate from the **Modif** indicator that indicates whether the entry was ever modified from or added to the default PPT. For example, the preceding settings for ERBMFMFC and ERB3GMFC (for example, RMF™) are the defaults on the OS level being examined, yet **Modif** shows that the entry was modified, due to an explicit specification in a SCHED*xx* member in parmlib.

The PPT detail display is shown in Figure 349 on page 470.

```
Program Property Table                                          Line 1 of 13
Command ===> _____________________________________________ Scroll===> CSR_
                                          26 Aug 1997 00:05
   Complex  System   Count Audit concerns Priority
   C#M4     C#M4        55             54        8
   Pri Program  Key Bypass NoDSI Modif NonSwap NonCan Priv Systask Audit concer
    3 COFMISDO   0 Bypass NoDSI       NonSwap NonCan      Systask Bypasses SAF

Program name (must be APF)    COFMISDO
Job step storage key            0
Bypass password / SAF         Yes
No dataset integrity          Yes
Default entry IEFSDPPT        Yes
Non-swappable                 Yes
Non-cancellable               Yes
Privileged (no SWAP)          No
System task not timed         Yes

Audit concern
Bypasses SAF (IBM default), Executes in system key (IBM default), No dataset
integrity (IBM default)
****************************** Bottom of Data ********************************
```

Figure 349. Program Property Table detail display

The detail display does not contain additional fields.

SVC - Supervisor Call report

The SVC report displays the Supervisor Calls and Extended Supervisor Routers (ESRs).

This report is available on a live system. Consequently, no CKFREEZE file is required.

Background

A SuperVisor Call (SVC) is an instruction that can be used by authorized and unauthorized programs to call a system function. The system contains an SVC*table* with information on all SVCs defined. The SVC instruction contains an SVC*number* that determines the SVC table entry to be used. The entry defines how control is to be transferred by the SVC instruction; that is, to which address and under which locks control is transferred. An SVC routine always receives control in Supervisor state, key 0.

An SVC table entry can contain the APF bit. If it is on, APF authorization is required to execute the SVC.

An SVC entry can be marked with the ESR bit. In this case, the address in the routine identifies a second-level SVC table called the ESR table. The system uses the contents of register 15 (called the *ESR number*) to identify the SVC table entry in this secondary table.

SVC routines must be in common storage to be callable from all address spaces.

The SVC table can be updated using the SVCUPDTE service. The SVCUPDTE service keeps track of the last update to the SVC in the SVC update table. Security zSecure reports on updates both with and without SVCUPDTE.

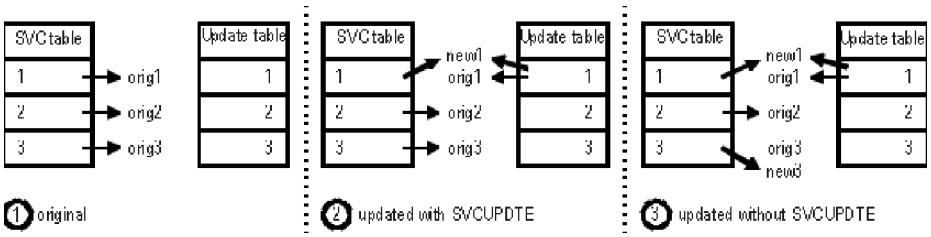


Figure 350. SVC updates

Auditing supervisor calls

The Supervisor Call routine is executed with the highest system authority, and can be called by any program if the APF bit in the SVC table is off. Because of this authority, SVC routines should take care not to introduce security leaks into the system by allowing a user more latitude than he should have according to the site security policy.

Regretfully, SVC routines exist that were built without adhering to the IBM guidelines or consulting a security expert. Most important features of such SVCs are that they can easily crash the system and that they can be used by system experts to circumvent all access control measures implemented in the operating system software.

On average, IBM SVCs tend to be safer than third-party vendor and site-designed SVC routines. Because of this, non-standard or front-ended SVC routines receive a higher audit priority than standard SVCs.

The batch sample to review the SVCs is CKALSVC, which produces three reports (two overview and one detailed report). The interactive reports are called CKADSVC0 (concise) and CKADSVC (detailed).

Note: The following information shows the concise version of the SVC report and then provides a description of the detailed report.

The concise SVC overview display is shown in Figure 351.

```
Supervisor Call Audit (concise)                                  Line 1 of 141
Command ===> _____________________________________________ Scroll===> CSR_
scroll right for more info                        5 Sep 2000 00:07
   Complex  System   Routines SVCs ESRs Audit concerns Priority
   DINO     DINO          141  104   37            133       18
   Pri SVC ES# APF Function                          Where   Entry at
__  18  83     Yes SMFWTM                            ECSA
s_  17 144     No  OpenEdition PTRACE debugging      EPLPA   IGC0014D in BPXINLP
__  16  51     No  SNAP/SNAPX/SDUMP/SDUMPX           EPLPA   IGC0005A
__  11  12     No  SYNCH/SYNCHX                      ENUC RO CSVSYNCH in IEANUC0
__  11  13     No  ABEND                             EPLPA   IGC0101C
__  11  46     No  TTIMER/STIMERM                    ENUC RO IGC046 in IEANUC01
__  11  47     No  STIMER/STIMERM                    ENUC RO IGC047 in IEANUC01
__  11  48     No  DEQ                               ENUC RO IGC048FP in IEANUC0
__  11  56     No  ENQ/RESERVE                       ENUC RO IGC056FP in IEANUC0
__  11 109  11 No  SDSF                              EMLPA   IGX00011
```

Figure 351. SVC overview display (concise)

The display shows the SVCs defined in the system, sorted in order of audit priority. It can be scrolled left and right to view additional information. The display contains the following fields of interest:

Table 234. SVC overview display (concise) - field descriptions

Field	Explanation
Complex	Name of the complex examined.
System	Name of the system examined.
Routines	The number of SVC and ESR routines found.
SVCs	The number of SVC routines found.
ESRs	The number of ESR routines found.
Audit concerns	The number of routines with audit concerns.
Priority	The highest audit priority found.
Pri	The audit priority.
SVC	The SVC number.
ES#	The ESR number.
APF	Indicates whether the caller must be APF-authorized.
Function	The documented function name of the SVC.
Where	SVC routine residency.
Entry at	Module and offset information.
Result	The result of an SVC disassembly.
Audit concern	Audit concerns identified.

The concise detail display is shown in Figure 352. The only additional information shown is the application to which the SVC belongs, if known. (Typically, this is not known for installation-defined SVC routines.)

```
Supervisor Call Audit (concise)                                  Line 1 of 5
Command ===> _____________________________________________ Scroll===> CSR_
scroll right for more info                      5 Sep 2000 00:07
   Complex  System   Routines SVCs ESRs Audit concerns Priority
   DINO     DINO          141  104   37            133       18
   Pri SVC ES# APF Function                          Where   Entry at
    17 144     No  OpenEdition PTRACE debugging     EPLPA   IGC0014D in BPXINLP
Appl     Result
OMVS
Audit concern
Updated using SVCUPDTE, IBM-range SVCno, Caller may be unauthorized
****************************** Bottom of Data ********************************
```

Figure 352. SVC detail display (concise)

The next set of displays shows the detailed SVC report. You are advised to skip these displays, and use concise reporting, until you are familiar with SVC routines in general and the SVC routines on your system in particular. The SVC overview display is shown in Figure 353 on page 473.

```
Supervisor Call Audit Display                                    Line 1 of 141
Command ===> _____________________________________________ Scroll===> CSR_
scroll right for more info                      5 Sep 2000 00:07
   Complex  System   Routines SVCs ESRs Audit concerns Priority
   DINO     DINO          141  104   37            133       18
   Pri SVC ES# APF Where    K SP  Program  U Sf InstrSc Function
__  18  83     Yes ECSA     0 241          2            SMFWTM
s_  17 144     No  EPLPA          IGC0014D 1            OpenEdition PTRACE debu
__  16  51     No  EPLPA          IGC0005A 1      M     SNAP/SNAPX/SDUMP/SDUMPX
__  11  12     No  ENUC RO        CSVSYNCH        M     SYNCH/SYNCHX
__  11  13     No  EPLPA          IGC0101C      A M0    ABEND
__  11  46     No  ENUC RO        IGC046           0    TTIMER/STIMERM
__  11  47     No  ENUC RO        IGC047           0    STIMER/STIMERM
__  11  48     No  ENUC RO        IGC048FP        M     DEQ
__  11  56     No  ENUC RO        IGC056FP        M     ENQ/RESERVE
__  11 109  11 No  EMLPA          IGX00011        M0    SDSF
```

Figure 353. SVC Call Audit display

The overview display contains the following fields of interest:

Table 235. SVC Call audit display - field descriptions

Field	Explanation
Complex	Name of the system examined.
System	Name of the system examined.
Routines	The number of SVC and ESR routines found.
SVCs	The number of SVC routines found.
ESRs	The number of ESR routines found.
Audit concerns	The number of routines with audit concerns.
Priority	The highest audit priority found.
Pri	The audit priority of the SVC routine.
SVC	The SVC number.
ES#	The ESR number.
APF	Indicates whether the caller must be APF-authorized.
Where	SVC routine residency.
K	SVC routine storage area key.
SP	SVC routine storage area sub-pool.
Program	The SVC routine module name.
U	The number of times the SVC routine was updated using SVCUPDTE.
Sf	The parmlib member IEASVCxx suffix used in the last SVCUPDTE call.
InstrSc	The results of an Instruction Scan.
Function	The documented function name of the SVC.
Eye catchers	In storage eye catchers for the SVC routine.
Result	The result of an SVC disassembly.
Str	Indicates whether a string scan resulted in a hit.
SVC scan result	Indicates whether a SVC call scan resulted in a hit.
SVC same as	The number of the first SVC sharing the same code.
Audit concern	Audit concerns identified.

Select any SVC for a detail display.

```
Supervisor Call Audit Display                                    Line 1 of 31
Command ===> _____________________________________________ Scroll===> CSR_
scroll right for more info                    5 Sep 2000 00:07
   Complex  System   Routines SVCs ESRs Audit concerns Priority
   DINO     DINO          141  104   37            133       18
   Pri SVC ES# APF Where    K SP  Program  U Sf InstrSc Function
    17 144     No  EPLPA          IGC0014D 1            OpenEdition PTRACE debu
Idx  Where   Key SP  Program  InstrSc Eye catchers
CN I EPLPA           IGC0014D         ..BPXNP14D09/14/98 HBB6608BPXINLPA..0By..
  O  NUC RO          IGCERROR         ..\n4.. 0o..o=o ..
Appl     Result
OMVS
SVCUPDTE Sf Last update Caller   Where   Module
       1    21 Aug 2000 8A0A0D06 EPVT
Index    Typ APF ESR Att Locks
Current: 3/4 No  No
Old:       2 No  No
Expect:  3/4 No  No  ??? ???
Instruction/Str/SVC scan results
           No
Audit concern
Updated using SVCUPDTE, IBM-range SVCno, Caller may be unauthorized
First 256 bytes of SVC
0000. 05F047F0 F0260000 C2D7E7D5 D7F1F4C4 *.0.00...BPXNP14D*
0010. F0F961F1 F461F9F8 40C8C2C2 F6F6F0F8 *09/14/98 HBB6608*
0020. C2D7E7C9 D5D3D7C1 B24000E0 B2190000 *BPXINLPA. .\....*
```

Figure 354. SVC Call Audit detail display

The detail display contains the following fields of interest:

Table 236. SVC Call Audit detail display - field descriptions

Field	Explanation
Idx	An index indicating the *versions* of the SVC grouped on one line. The index can be any of the following: C is current N result of last update O the version prior to the last update I the expected routine based on the module name The fields on the rest of the line all describe the same version of the SVC.
Where	SVC routine residency.
Key	SVC routine storage area key.
SP	SVC routine storage area sub-pool.
Program	SVC routine module name.
InstrSc	Results of an instruction scan.
Eye catchers	In storage eye catchers.
Address	SVC routine address.
Length	Approximate length of the SVC routine.
Entry at	Module and offset information.
SVC same as	Lowest SVC and optionally ESR number with the same address.
Result	Result of SVC code disassembly.
Appl	Application the SVC belongs to.
Result	Result of disassembly of current SVC.

Table 236. SVC Call Audit detail display - field descriptions (continued)

Field	Explanation
SVCUPDTE	Number of updates made using SVCUPDTE.
Sf	PARMLIB member IEASVCxx suffix used in SVCUPDTE call.
Last update	Date of last SVCUPDTE call.
Caller	Address of last caller of SVCUPDTE.
Where	Last SVCUPDTE caller's residency.
Module	Last SVCUPDTE caller's module information.
Index	An index indicating the version of the SVC for which the type is shown on the line, one of Current (from SVC table). Old (from SVCUPDTE table), Expected (from documentation).
Typ	SVC type. This can be 1, 2, 3/4, or 6. The SVC type determines the load module naming convention.
APF	Indicates whether APF-authorization is required to call the SVC.
ESR	Indicates whether the SVC is an ESR.
Att	SVC attributes. N for non-preemptive, S for assisted, and A for AR mode.
Locks	SVC locks. C for CMS lock, D for DISP lock, L for LOCAL lock, O for OPT lock, and S for SALLOC lock.
Instr/Str/SVC	Results of instruction, String, and SVC scans.
Audit concern	Audit concerns identified.
First 256 bytes of SVC	The start of the SVC is shown both in hex and text. Nonprintables have been replaced with periods in the latter.

PC - Program Call report

The Program Call report displays the Program Call routines, their entry tables, and the connected address spaces.

The report requires a CKFREEZE file made in an APF-authorized run of zSecure Collect.

Background

The Program Call (PC) is a more modern alternative to the SVC (Supervisor Call). (In fact, IBM urges vendors to use PC instead of SVC because it is more efficient.) Program Calls are instructions for calling a routine outside the current program. The routine can be executed in another address space and with different authorization.

The Program Call instruction accepts a PC *number* that determines the routine to be called. The first part of the number is the *Linkage Index* LX that determines the address of an *Entry Table* ET . The second part is the *Entry Table Index* EX that identifies an entry in the entry table.

The entry defines the address, the address space, and the authorities used when control is to be transferred by the PC instruction.

An entry table can be shared between address spaces. MVS tries to keep the linkage index the same for all address spaces sharing an entry table, but this is not a hardware requirement. If an entry table is to be shared between all address

spaces, MVS allows allocation of a *system* LX to this entry table. A non-system LX/entry table can only be used from address spaces explicitly *connected* to the entry table.

The Entry Table entry can define the following features:

1. The address space where to execute the PC routine (may be the current address space).
2. Supervisor mode or Problem program mode.
3. The Program Status Word (PSW) protection key that the Program Call runs in. This key determines the memory that may be accessed by the PC routine. A key in the range 0 to 7 makes the PC routine authorized.
4. The set of PSW keys the routine may switch to (the EKM or Entry Key Mask). One or more keys in the range 0 to 7 make the PC routine authorized.
5. Whether the EKM is replacing or expanding the current authority.
6. The set of PSW keys that authorize use of this entry (the AKM or Authorized Key Mask).
7. The address of the LPA Latent Parameter Area . In MVS this is a 16 byte area that contains linkage stack origins and 2 user fullwords.

Many MVS functions have been coded to be independent of the actual PC number assigned. This is accomplished by loading the actual PC number from a certain offset in the System Function Table or SFT.

Each Program Call can have a *Latent Parameter Area* (LPA, not to be confused with the link pack area). This is an area at a location fixed when the PC was created. In this area, there are two 4-byte fields available for use by the PC routine. Most PCs do not use these fields, or use them to store simple values. However, some PCs use these fields to store one or two pointers to larger parameter areas. The Latent Parameter Area is shown in Figure 355.

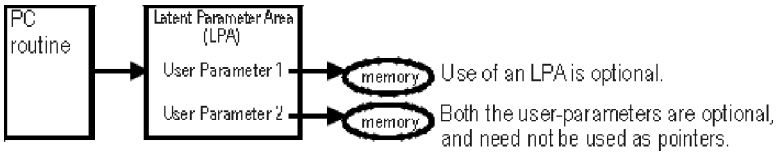


Figure 355. PC Latent Parameter Area

Security zSecure tries to trace the LPA pointers, to see if they point to common storage. If any of these pointers appears to point to *writable* common storage, Security zSecure warns you because there is a chance that any user can overwrite parameters or storage used by the Program Call.

Theoretically, an entry table can have different linkage indices in different address spaces; as a result, the same PC routine, with the same parameters, would have several different PC numbers. This is illustrated in Figure 356 on page 477.

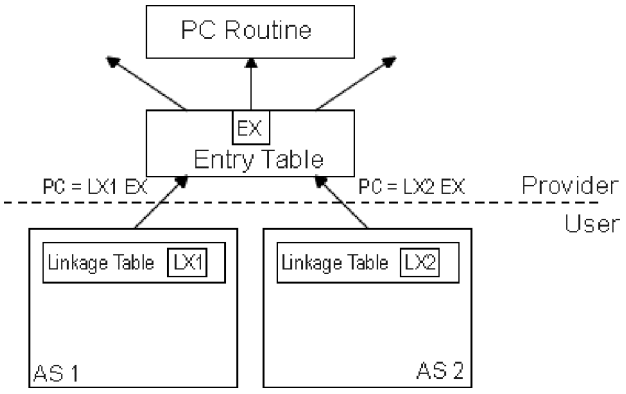


Figure 356. Program Call with more than one LX

However, MVS tries to prevent this situation from occurring. Security zSecure is able to report these cases correctly. (No audit concern is generated.)

Auditing Program Calls

Compared with Supervisor Calls (SVCs), the PC allows more precise control over authorities required and obtained. However, the same kind of audit concerns apply as for SVCs.

The PC routines requiring most audit attention are the routines that:

- Can be executed from any address space (that is, routines that reside in a system Entry Table).
- Can be called by unauthorized programs (the AKM contains key 8).
- Run authorized (that is, routines that run in supervisor state, add a system key to the EKM, or have a system key as EK).
- Reside in globally readable common storage or libraries (allowing uncontrolled disassembly).
- Reside in private storage (PVT or EPVT), but are not space-switching. Each caller can execute a different version of the Program Call.

  If the Program Call executes authorized and the caller can be unauthorized, a Program Call in the (E)PVT might allow any user to gain authorization.
- Have an LPA with user-pointers pointing to writable common storage.

The batch sample to review the Program Calls is CKALSPC, which produces six batch reports, including overview and detailed reports. The interactive reports are called CKADSPC0 (concise) and CKADSPC (detailed).

Note: The following information first shows the concise version of the Program Call report, and then describes the detailed report.

The concise ISPF Program Call report is split into four levels. The first level shows the number of system-wide and non-system-wide program calls per system analyzed, and the highest audit priority identified, as shown in Figure 357 on page 478.

```
Program Call Audit (concise)                                    Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR_
scroll right or select for more info          11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
s_ DINO     DINO     Systemwide   605            605       13
__ DINO     DINO                   34             34        3
****************************** Bottom of Data ********************************
```

Figure 357. Program Call first-level display (concise)

The first-level display contains the following fields of interest:

Table 237. Program Call Audit - field descriptions

Field	Explanation
Complex	The complex name.
System	The system name.
Systemwide	Indicates whether the program call is available system-wide.
PCs	The number of Program Calls.
Audit concerns	The number of Program Calls with an audit-concern identified.
Priority	The highest audit priority found.

In the display in Figure 357, the highest audit priority was found among the system-wide Program Calls. Selecting that row shows the second-level display, see Figure 358.

```
Program Call Audit (concise)                                   Line 1 of 48
Command ===> _____________________________________________ Scroll===> CSR_
scroll right or select for more info          11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
   DINO     DINO     Systemwide   605            605       13
   Priority ET-owner Connects     PCs Audit concerns
s_       13 VMCF                   21             21
__        9 *MASTER*               6              6
__        9 PCAUTH                 78             78
__        8 CONSOLE                20             20
__        8 GRS                    26             26
__        5 *MASTER*               2              2
```

Figure 358. Program Call second-level display (concise)

The second-level display summarizes the system-wide Entry Tables (ETs). For each entry table, it shows the owning address space, the number of ET connections (blank for a system-wide ET), and the number of Program Calls defined in the entry table.

Select any row for an overview of the Program Calls defined in the ET.

```
Program Call Audit (concise)                                    Line 1 of 21
Command ===> _____________________________________________ Scroll===> CSR_
scroll right or select for more info          11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
   DINO     DINO     Systemwide   605            605       13
   Priority ET-owner Connects     PCs Audit concerns
         13 VMCF                   21             21
   Pr PCnumber Aut Caller   Runs in  Description                 Where   Entry
__ 13 00210D   Yes                                               EPVT
__ 13 002111   Yes                                               EPVT
s_  4 002100   No                    (Communications Server for z  EPLPA   MVPYV
__  4 002102   No                    (Communications Server for z/ EPLPA   EZAYV
__  4 002103   No           VMCF                                 EPVT
__  4 002104   No                    (Communications for z EPLPA   MVPYS
__  4 002105   No           VMCF                                 EPVT
__  4 002108   No           VMCF                                 EPVT
__  4 00210A   No           VMCF                                 EPVT
__  4 00210B   No           VMCF                                 EPVT
__  4 00210E   No           VMCF                                 EPVT
__  4 00210F   No                    (Communications for z EPLPA   MVPYI
__  4 002113   No                    (Communications for z EPLPA   MVPYS
__  3 002101   Yes          VMCF                                 EPVT
__  3 002106   Yes          VMCF                                 EPVT
__  3 002107   Yes          VMCF                                 EPVT
__  3 002109   Yes          VMCF                                 EPVT
__  3 00210C   Yes          VMCF                                 EPVT
__  3 002110   Yes          VMCF                                 EPVT
__  3 002112   Yes          VMCF                                 EPVT
__  3 002114   Yes          VMCF                                 EPVT
****************************** Bottom of Data ********************************
```

Figure 359. Program Call overview display (concise)

The Program Call overview display shows the PCs defined in a single Entry Table, sorted by audit priority. It can be scrolled left and right to view additional information. The display contains the following fields of interest:

Table 238. Program Call Audit - field descriptions

Field	Explanation
Pr	The audit priority.
PCnum	The Program Call number of the PC routine.
Aut	Indicates whether the caller of the PC routine must be authorized.
Caller	The job name of the address space connected to the PC (blank: available system-wide, or no connections). The value <more>indicates several callers were identified; these are all listed on the detail panel.
Runs in	The job name of the address space in which the PC runs, if it is a space-switching PC. This field is blank for non-space-switching PCs, as these execute in the caller's address space.
Description	Description of the PC, based on the index in the SFT, or a guess based on the module name. In the latter case, the description is surrounded by parentheses.
Where	The residency of the Program Call routine.
Entry at	Module information and offset.
Audit concern	Audit concerns identified.

Select any PC entry on the overview panel for a detailed view. The detailed view does not add additional fields; for a non-system-wide PC, all callers are listed. The

detail display is shown in Figure 360.

```
Program Call Audit (concise)                                    Line 1 of 3
Command ===> ____________________________________________ Scroll===> CSR_
scroll right or select for more info           11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
   DINO     DINO     Systemwide   605            605       13
   Priority ET-owner Connects     PCs Audit concerns
         13 VMCF                   21             21
   Pr PCnumber Aut Caller   Runs in  Description                 Where   Entry
    4 002100   No                   (Communications for z EPLPA   MVPYV
PCnumber Caller   Description
002100            (Communications for z
Audit concern
Executes authorized, Caller may be unauthorized, Globally callable
****************************** Bottom of Data ********************************
```

Figure 360. Program Call detail display (concise)

The next set of displays shows the detailed Program Call report. You are advised to skip these displays, and use concise reporting, until you are familiar with Program Calls in general and the PCs on your system in particular. For clarity, the same system and PC routines are examined as in the concise displays above.

The Program Call first-level display is shown in Figure 361.

```
Program Call Audit Display                                      Line 1 of 2
Command ===> ____________________________________________ Scroll===> CSR_
scroll right or select for more info           11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
s_ DINO     DINO     Systemwide   605            605       13
__ DINO     DINO                   34             34        3
****************************** Bottom of Data ********************************
```

Figure 361. Program Call first-level display

It contains the same fields as the concise first-level display.

In the display in Figure 361, the highest audit priority was found among the system-wide Program Calls. Selecting that row shows the second-level display, which is identical to the concise version except for the title. Selecting a row there shows the overview display.

```
Program Call Audit Display                                      Line 1 of 21
Command ===> _____________________________________________ Scroll===> CSR_
scroll right or select for more info          11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
   DINO     DINO     Systemwide   605            605       13
   Priority ET-owner Connects     PCs Audit concerns
         13 VMCF                   21             21
   Pr PCnumber A Caller   AKM  Runs in  M K oEKM  T Where   Program  Eye catche
__ 13 00210D   Y          8000|          S   o8000 b EPVT              ..}{qq..{{
__ 13 002111   Y          8000|          S   o8000 b EPVT              ..P
s_  4 002100   N          FFFF|          S   o8000 b EPLPA   MVPYVMC  .006.MVPYV
__  4 002102   N          FFFF|          S   o8000 b EPLPA   EZAYVMCF ..MVPYSSM
__  4 002103   N          FFFF|VMCF      S   o8000 b EPVT              ..\Kd..Kh
__  4 002104   N          FFFF|          S   o8000 b EPLPA   MVPYSSM2 ..
__  4 002105   N          FFFF|VMCF      S   o8000 b EPVT              ..\Kd..
__  4 002108   N          FFFF|VMCF      S   o8000 b EPVT              ..\Kd..0
__  4 00210A   N          FFFF|VMCF      S   o8000 b EPVT              .006.MVPXI
__  4 00210B   N          FFFF|VMCF      S   o8000 b EPVT              .006.MVPXU
__  4 00210E   N          FFFF|VMCF      S   o8000 b EPVT              ..}{qq..{{
__  4 00210F   N          FFFF|          S   o8000 b EPLPA   MVPYIUC  .006.MVPYI
__  4 002113   N          FFFF|          S   o8000 b EPLPA   MVPYSSM3 ..0
__  3 002101   Y          8000|VMCF      S   o8000 b EPVT              ..MVPXVMC
__  3 002106   Y          8000|VMCF      S   o8000 b EPVT              ..MVPXSSM
__  3 002107   Y          8000|VMCF      S   o8000 b EPVT              ..\Kd..P
__  3 002109   Y          8000|VMCF      S   o8000 b EPVT              ..\Kd..
__  3 00210C   Y          8000|VMCF      S   o8000 b EPVT              .006.MVPXT
__  3 002110   Y          8000|VMCF      S   o8000 b EPVT              ..MVPXIUC
__  3 002112   Y          8000|VMCF      S   o8000 b EPVT              ..
__  3 002114   Y          8000|VMCF      S   o8000 b EPVT              ..\Kd..0
******************************* Bottom of Data ********************************
```

Figure 362. Program Call overview display

The overview display can be scrolled right repeatedly to show more information; these fields are repeated on the detail display of any one Program Call. The overview display contains the following fields of interest:

Table 239. Program Call Audit display - field descriptions

Field	Explanation
Pr	The audit priority.
PC num	The Program Call number of the PC routine.
A	Indicates whether the caller of the PC routine must be authorized (Y) or not (N).
Caller	The job name of the address space connected to the PC (blank: available system-wide, or no connections). The value '<more>' indicates several callers were identified; these are all listed on the detail panel.
AKM	The authorized key mask, a bit field indicating the PSW keys that a caller can have.
Runs in	The job name of the address space in which the PC runs, if it is a space-switching PC.
M	The mode in which the PC runs: supervisor state (S) or problem-program mode (P).
K	Indicates the PSW key that the PC runs in. Keys in the range 0 to 7 imply authorization.
oEKM	Five character field where the first character indicates how the PC runs with the caller's key: • Mask OR-ed with the Entry Key Mask EKM (O). • EKM replaces the caller's key mask (R) The remaining four characters indicate the EKM used.

Table 239. Program Call Audit display - field descriptions (continued)

Field	Explanation
T	The type of the PC: basic (B) or space-switching (S).
Where	The residency of the Program Call routine.
Program	The module name of the Program Call routine.
Eye catchers	Visible eye catchers from the Program Call routine.
Address	Program Call routine entry point.
Where	Program Call routine residency.
Entry at	Module information and offset.
Length	Approximate length of the Program Call code.
AM	Addressing mode.
InstrSc	Instruction scan hits.
Str	String scan hits.
LPArea	Residency of the Latent Parameter Area (LPA).
K	Storage protection key of the LPA memory area, LPA param1/param2 area.
SP	Sub-pool of the LPA memory area, LPA param1/param2 area.
Px area	Residency of the LPA param1/param2 area.
SFT	Index of the PC code in the System Function Table (SFT).
Description	Description of the PC, based on the index in the SFT, or a guess based on the module name. In the latter case, the description is surrounded by parentheses.
Audit concern	Audit concerns identified.

On the overview display, select any line for a detailed display of the Program Call.

```
Program Call Audit Display                                      Line 1 of 33
Command ===> _____________________________________________ Scroll===> CSR_
scroll right or select for more info           11 Sep 2006 00:07
   Complex  System   Systemwide   PCs Audit concerns Priority
   DINO     DINO     Systemwide   605            605       13
   Priority ET-owner Connects     PCs Audit concerns
         13 VMCF                   21             21
   Pr PCnumber A Caller   AKM  Runs in  M K oEKM  T Where   Program  Eye catche
    4 002100   N          FFFF         S   o8000 b EPLPA   MVPYVMC  .006.MVPYV
PCnumber LX-seqno Caller   ASID Dorm  -LX- Syst LX-owner ASID  SFT Description
002100                     0000 No      33 Yes  VMCF     002A      (Communicati
PSW Mode   Key Type                   -EX- Syst ET-owner ASID Connects
SUPERVISOR     BASIC                     0 Yes  VMCF     002A
Authorized Key Mask
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Entry Key Mask / usage
0 OR
Storage area          Address  Where   Key SP  Length AM Module
PC routine:           067EDD40 EPLPA             2104 31 MVPYVMC in EZAYVMCF
Latent Parm:          02CF6000 ESQA     0 245
User parm 1:          00C1B420 CSA      0 241
User parm 2:
Instruction/Str/SVC scan results
            No
Audit concern
Executes authorized, Caller may be unauthorized, Globally callable
First 256 bytes of PC routine
0000. 05F047F0 F0F612D4 E5D7E8E5 D4C34040 *.0.006.MVPYVMC  *
0010. 40F2F0F0 F14BF1F1 F0D38983 8595A285 * 2001.110License*
0020. 8440D481 A3859989 8193A240 6040D799 *d Materials - Pr*
```

Figure 363. Program Call Detail Display

The detail display contains the following fields of interest:

Table 240. Program Call Audit display - field descriptions

Field	Explanation
PC num	All Program Call numbers by which the PC routine can be called.
LX-seqno	The sequence number for a reused Linkage Index. To be used to verify whether a PC instruction was intended for the current incarnation of the LX.
Caller	The job names of all connected address spaces.
ASID	Address space ID of all connected address spaces.
Dorm	Indicates whether the LX connect is dormant or not.
LX	The Linkage Index of the Entry Table of the Program Call.
Syst	Indicates whether the Linkage Index is a system index.
LX-owner	The job name of the Linkage Index owning address space.
ASID	The Address Space ID of the Linkage Index owner.
SFT	The index in the System Function Table.
Description	Description of the PC, based on the index in the SFT, or a guess based on the module name. In the latter case, the description is surrounded by parentheses.
PSW Mode	Indicates the state in which the PC runs (Supervisor or Problem-program mode).
Key	The PSW key in which the PC routine executes.
Type	The type of PC routine (Stacking or Basic).
EX	The index of the PC in the Entry table.
Syst	Indicates whether the Entry Table is a system entry table.

Table 240. Program Call Audit display - field descriptions (continued)

Field	Explanation
ET-owner	The job name of the Entry Table owning address space.
ASID	The Address Space id of the Entry Table owner.
Connects	The number of address spaces connected to the Entry Table (blank for a system ET).
Authorized Key Mask	A list of the PSW keys that a caller can have.
Entry Key Mask	A list of the keys in the Entry Key Mask EKM.
usage	Indicates whether the EKM is OR-ed with the caller's key mask, or REPLACEs it.
Storage area	Which storage area is described on this line (PC routine, latent parameter area, or LPA param1/param2).
Address	The address of the PC routine, latent parameter area, and LPA param1/param2.
Where	The residency of the PC routine, latent parameter area, and LPA param1/param2.
Key	The storage area key of the PC routine, latent parameter area, and LPA param1/param2.
SP	The storage area subpool of the PC routine, latent parameter area, and LPA param1/param2.
Length	Approximate length of the PC routine.
AM	Addressing mode.
Module	Module name of the PC routine.
Instr/Str/SVC Scan	Results of instruction, string, and SVC scans.
Audit concern	Audit concerns identified.
First 256 bytes of PC routine	The start of the PC routine is shown both in hex and text. In the text, values that cannot be printed have been replaced with periods.

TAPE - Tape protection settings

The TAPE report shows the effective tape settings. It also shows CA-1 specific settings.

The report requires a CKFREEZE file made in an APF-authorized run of zSecure Collect.

Documentation for each of the fields displayed can be found in the language reference for the SYSTEM NEWLIST in Chapter 13, “SELECT/LIST Fields,” on page 953.

Figure 364 on page 485 shows a sample Tape protection settings display.

```
Tape protection settings (RACF)                              Line 1 of 13
Command ===> _____________________________________________ Scroll===> CSR
                                                 06 Sep 2006 14:18
   Complex  System   Collect time stamp
   C#MF07#4 OR37     05 Sep 2006 14:18


DFP tape protection settings            CA1 specific settings
Tape use DATASET  TAPEAUTHDSN No                          CA1 OPEN/CLOSE/EOV chk  OCEOV Yes
Tape file1 check   TAPEAUTHF1 No                          CA1 first file check     DSNB Yes
Tape undef result TAPEAUTHRC4 FAIL                        CA1 SVC access check     YSVC No
Tape fail result  TAPEAUTHRC8 FAIL                        CA1 TMC & DSNB rec chk  BATCH Yes
                                                          CA1 Online user pswd chk PSWD Yes
RACF tape protection settings   CA1 Function call check  FUNC Yes
Tape dataset check TAPEDSN    Yes                         CA1 Undefined FAIL      UNDEF Yes
Tape volume protection active Yes                         CA1 CREATE access lvl  CREATE UPDATE
Protection duration RETPD     0000                        CA1 Foreign DSN check FORNDSN ALL
                                                          CA1 Data set erase        DSE No
****************************** Bottom of Data ********************************
```

Figure 364. Tape protection settings display

IOAPP - I/O Appendage report

The I/O appendage report describes the authorized I/O appendages table.

This report is available on a live system (no CKFREEZE file is required).

Background

I/O appendages are exit routines that receive control during certain stages of an I/O operation. They are entered in supervisor state.

Appendages are identified by a two-character identifier, that is passed to OPEN as part of the Data Control Block (DCB) describing the file to be opened.

OPEN tries to locate a module named IGG019nn where *nn* is the appendage id. Just naming the module this way is not enough, it looks for a module that:

1. Resides in an authorized library (the Authorization Code of the module is not checked, hence AC=0 is sufficient and desirable).
2. Has the RENT attribute - it must be reenterable.

If these conditions are not met, the operation is stopped using abnormal end code 806.

An appendage that is part of the authorized appendage table can be requested by an unauthorized user, and runs in supervisor state. Hence, the appendage can bypass access controls, and should contain extensive authorization checking code if it is used to do exactly that.

In the past, End-of-extent appendages that reset the extents from the actual data set boundaries to the complete volume have been a popular way for DASD management packages to obtain access to the complete volume. Such an appendage is a security exposure if it is added to the authorized I/O appendage table, since it bypasses data set access control.

The I/O appendage parameters are specified in parmlib member IEAAPP00.

Auditing I/O appendages

The following considerations apply when auditing I/O appendages:

- All appendages in the table should be reviewed to check that they are indeed properly designed for use by unauthorized programs.
- Prior to DFSMS 1.4, there is one entry automatically added by MVS, which is E4 (channel end/abnormal end appendage for interactive terminal facility, or IGG019E4). Verify that IGG019E4 appendage present in the system is valid and has not been replaced by an invalid, potentially malicious version.

The batch report to review the I/O appendages is CKALSIOA. The interactive report is called CKADSIOA.

For more information on any I/O appendage resident in-storage, see the exit report.

Sample ISPF overview and detail displays for the I/O appendage report are shown in the following figures.

```
Authorized I/O Appendage table                                  Line 1 of 5
Command ===> ____________________________________________ Scroll===> CSR_
                                                 10 Oct 1994 11:27
   Complex  System   Appendages Audit concerns Priority
   IPO1     3090              5              4       20
    Pri Id Typ
S_  20  XX ABE

           Non-default Appendage
           00CFE000 PLPA    ..
__  20  XY ABE

           Non-default Appendage
           00CF6000 PLPA
__  20  Z8 CHE ABE

           Non-default Appendage
           00F06708 PLPA
__  20  Z9 CHE ABE

           Non-default Appendage
           00CD6000 PLPA
__      E4 CHE ABE
           Interactive Terminal Facility CHE/ABE Appendage
           Added automatically by MVS

****************************** Bottom of Data ******************************
```

Figure 365. I/O Appendage Overview Display

The overview panel displays the I/O appendages and their types, a description, and an audit concern; select any row for a detail display.

```
Authorized I/O Appendage table                                    Line 1 of 13
Command ===> _____________________________________________ Scroll===> CSR_
                                                 10 Oct 1994 11:27
   Complex  System   Appendages Audit concerns Priority
   IPO1     3090              5              4       20
Pri Id Typ
20 XX ABE
Appendage ID                  XX
Appendage type                ABE Abnormal End
Conforms to default           No
Appendage description
Module name loaded by OPEN    IGG019XX
Entry point if resident       00CFE000
Appendage residency           PLPA
Browse of appendage code      j.....n....=...x........n.....0.O...........K...{

Audit concern
Non-default Appendage
****************************** Bottom of Data ********************************
```

Figure 366. I/O Appendage Detail Display

A sample batch report is shown in Figure 367

```
I / O   A P P E N D A G E   T A B L E   10 Oct 1994 11:27
Authorized I/O Appendage table


Complex  System   Appendages Audit concerns Priority
IPO1     3090              5              4       20

 Pri Id Type                              Audit concern

  20 XX ABE Abnormal End                  Non-default Appendage

      00E62C38 PLPA    j.....n....=...x........n.....0.O...........K...{
  20 XY ABE Abnormal End                  Non-default Appendage

      00CE1000 PLPA
  20 Z8 CHE Channel End                   Non-default Appendage
        ABE Abnormal End

      00E70AA8 PLPA
  20 Z9 CHE Channel End                   Non-default Appendage
        ABE Abnormal End

      00D316D0 PLPA
     E4 CHE Channel End                   Added automatically by MVS
        ABE Abnormal End
      Interactive Terminal Facility CHE/ABE Appendage
```

Figure 367. Batch I/O Appendage report

The reports contain the following fields of interest:

Table 241. Batch I/O Appendage report - field descriptions

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Appendages	The number of I/O appendages.
Audit concerns	The number of I/O appendages for which audit concerns were identified.
Priority	The highest audit priority for any of the I/O appendages.
Pri	Audit priority. A higher number indicates greater concern.

Table 241. Batch I/O Appendage report - field descriptions (continued)

Field	Explanation
Id	The I/O appendage ID. When combined with the fixed prefix IGG019, this makes up the appendage load module name.
Type	The I/O event types for which the appendage can be used.
Audit concern	Audit concerns identified.
Description	Description of the I/O appendage.
Entry point	Address of the default I/O appendage routine (if the I/O appendage resides in-storage).
Residency	The virtual storage area where the appendage resides.
Eye catchers	The start of the I/O appendage, usually containing eye catchers.
Conforms to default	Indicates whether the appendage conforms to the default defined.

IPSTACK - Communications Server IP stack display report

The Communications Server IP stack display report lists the TCP/IP stack configuration settings.

The data for this report is only available if a `CKFREEZE` file has been created during an APF-authorized run of zSecure Collect (CKFCOLL) with option `TCPIP=YES`. For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

Detailed field information is available by pressing F1 on an IP report selection panel or on any field within a panel. Descriptions are also provided in the SELECT/LIST fields chapter. For the IP configuration data field names and descriptions for IP* NEWLIST types, see "IP: Profile information for TCP/IP configuration" on page 1054. For information on the IP configuration data fields used for SMF event reporting (SMF record 119, subtype 4), see "SMF: SMF records" on page 1276.

The batch report to review the IP stack is CKALSIP. The interactive report is called CKADSIP.

Sample overview and detail display panels for the Communications Server IP stack display report are shown in Figure 368 and Figure 369 on page 489.

```
                                                                Line 1 of 1
Communications Server IP stack display
Command ===> ____________________________________________________ Scroll===> CSR
                                              31 Aug 2011 10:57
   Complex  Sysplex  Syst     Stack    Count Audit concerns Priority
   NMPIPL87 PLEX1    IPO1     TCPIP        1              1       28
   Pri Stack    Start date and time     Dataset name (member)
    28 TCPIP    29Aug2011 01:33:30.79
```

Figure 368. Communications Server IP stack overview display

```
Communications Server IP stack display                          Line 1 of 55
Command ===> ____________________________________________________ Scroll===> CSR_
  All TCP/IP stack information                    6 Aug 2009 10:03
  Dataset name (member)
  shared.parmlib(tcpntw14)
  SHARED.PARMLIB(TCPIEZOS)
  System identification
  Complex name                  EZOS
  System SMF ID                 EZOS
  Sysplex name                  EZOSRD2R
  Sysplex group name            EZBTCPCS

  IP stack data                           Global configuration data
  Stack name                    TCPIP     QDIO VLAN id                      0
  TCP low ports restricted      No        Terminate if MLS check fails  No
  UDP low ports restricted      Yes       VTAM XCF group EZBTCP suffix
  Start date/time                9Jan2009 09:29:31.34
  Last change date and time     - ??? -
  Dataset name (member)         shared.parmlib(tcpntw14)
  Dataset name (member)         SHARED.PARMLIB(TCPIEZOS)
  TCP/IP stack source VIPA
  VIPA interface name (IPv6)

  IPSEC  data                             SACONFIG data
  Allow VIPA distr for tunnel   No        OSASF subagent port               0
  Honor IPSEC rule log setting  Yes       SNMP subagent port              161
  Log implicit default rules    No        Unsafe default SNMP password  Yes

  SMF record 119 logging                  NETMON  data
  SMF 119-1 TCP connection init Yes       Enable packet trace NMI       No
  SMF 119-2 TCP termination     No        Enable IPSEC NMI              No
  SMF 119-3 FTP client          Yes       Enable PROFILE NMI            No
  SMF 119-5 TCPIP statistics    Yes       Enable SMF NMI                No
  SMF 119-6 Interf. statistics  Yes       Minimum seconds TCP life NMI   0
  SMF 119-7 port statistics     Yes       Enable TCP connection NMI     No
  SMF 119-8 IP stack start/stop Yes
  SMF 119-10 UDP termination    No
  SMF 119-22/23 TN3270 client   No
  SMF 119-77/78/79/80 IP sec.   Yes

  IPCONFIG  data
  IPv4 configuration            FORMAT LONG
  IPv4 configuration            IGNOREDDIRECT configured
  IPv4 configuration            IGNOREDDIRECT actual
  IPv4 configuration            IPSECURITY
  V4 filtering and IPSEC tunnel Yes
  IPv6 configuration            DATAGRAMFWD
  V6 filtering and IPSEC tunnel No

  Dynamics XCF interface data
  Dynamic XCF interface ID
  Dyn XCF secur. class (IPv6)     0
  Dynamic XCF IPv4 subnet mask    0
  Dynamic XCF IP address (IPv4)
  Dyn XCF prefix length (IPv4)    0
  Dyn XCF secur. class (IPv4)     0
  Dynamic XCF IP address (IPv6)
  Dyn XCF prefix length (IPv6)    0
  Dyn XCF src VIPA interface
  Dyn XCF prefix length (IPv6)    0
  Dyn XCF src VIPA interface

Audit concern
No access control to/from foreign and local networks
 ******************************* Bottom of Data ********************************
```

Figure 369. IP Stack detail display

Auditing the IP stack

The following considerations apply when auditing the IP stack.

- Ports below 1024 should be reserved, so users and programs cannot bind to low TCP and UDP ports by default and masquerade as legitimate services.
- IPv4 and IPv6 IP filtering support and IPSec tunnel support should be active.
- The audit trail should show attacks stopped by filter rules, including default filter rules.
- The audit trail should show all SMF119, FTPCLIENT, IFSTAT, IPSECURITY, PORTSTAT, TCPINIT, TCPIPSTACK, TCPIPSTAT, TCPTERM, TN3270CLIENT, and UDPTERM records.
- There should be access control to and from foreign and local networks.
- Access control should be required to and from foreign networks.
- There should be access control within the local network.
- Even when IPSTACK shows no concern of users being able to modify TCP/IP security parameters, it is possible that certain users are able to do so. To show the access of individual users to sensitive resources, examine the following reports:
  - "TRUSTUSR - Trusted users report" on page 292
  - "SENSTRUS - Sensitive Data Trustees report" on page 317
- Denial-of-service attacks should be attributable to authenticated users.
- By default, no user should be able to read netstat ALL, ALLCONN, ARP, BYTEINFO, CACHINFO, CLIENTS, CONFIG, CONN, DEFADDRT, DEVLINKS, GATE, HOME, IDS, ND, PORTLIST, RESCACHE, ROUTE, SLAP, SOCKETS, SRCIP, STATS, TELNET, TTLS, UP, VCRT, VDPT, VIPADCFG, and VIPADYN output. Being able to read sensitive netstat data could facilitate mounting an attack.
- By default, no user should be able to control the TCP/IP security parameters in effect after the next stack setup modification.

  Even when IPSTACK shows no concern of users being able to control the TCP/IP security parameters in effect after the next stack setup modification, it is possible that certain users are able to do so. To show the access of individual users to sensitive resources, examine the TRUSTUSR - Trusted users report or the SENSTRUS - Sensitive Data Trustees report.

IPPORT - Communications Server IP ports display report

The Communications Server IP ports report describes the port configuration of TCP/IP stacks. The data for this report is only available if a `CKFREEZE` file has been created during an APF-authorized run of zSecure Collect with option `TCPIP=YES`. For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_PORT: TCP/IP port configuration" on page 1061.

The batch report to review the IP ports is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP ports report are shown in Figure 370 on page 491 and Figure 371 on page 491.

```
Communications Server IP ports display                          Line 1 of 33
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53
   Complex  Sysplex  Syst     Stack    Count Audit concerns Priority
   SYS1     PLEX1    IPO1     TCPIP       33             31       22
   Pri Stack    BPort EPort Prt Bind IP address replacement
__  22 TCPIP       21    21 TCP
__  22 TCPIP       23    23 TCP
__  22 TCPIP       80    80 TCP
__  22 TCPIP      111   111 TCP
__  22 TCPIP      111   111 UDP
__  22 TCPIP      161   161 UDP
__  22 TCPIP      162   162 UDP
__  22 TCPIP      623   623 TCP
__  22 TCPIP      750   750 TCP
__  22 TCPIP      750   750 UDP
__  20 TCPIP        7     7 TCP
__  20 TCPIP        7     7 UDP
__  20 TCPIP        9     9 TCP
__  20 TCPIP        9     9 UDP
__  20 TCPIP       19    19 TCP
__  20 TCPIP       19    19 UDP
__  20 TCPIP       20    20 TCP
__  20 TCPIP       25    25 TCP
```

Figure 370. IP ports overview display

```
Communications Server IP ports display                          Line 1 of 23
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53

 IP stack data
_ Complex name                 SYS1
_ Stack name                   TCPIP
_ System SMF ID                IPO1
  Sysplex name                 PLEX1

  PORT data
  Beginning port                  21 ftp
  End port                        21 ftp
  Bind IP address
  Port use restriction         JOBNAME
  Port count                   1
  Port options                 DELAYACKS
  PORTRANGE entry              No
_ Protocol                     TCP
  Secure unreserved ports      No
  SERVAUTH resource name

  Audit concern
```

Figure 371. IP ports detail display

Auditing the IP ports

The following considerations apply when auditing the IP ports.

- SAF parameters should prevent users and programs from binding to privileged ports. Being able to bind to a privileged port allows a user to masquerade as a legitimate service. For some ports it also allows one to receive passwords.

  Even when IPPORT shows no concern of users being able to bind to privileged ports, it is possible that certain users are able to do so. To show the access of individual users to sensitive resources, examine the following reports:

  – "TRUSTUSR - Trusted users report" on page 292
  – "SENSTRUS - Sensitive Data Trustees report" on page 317

IPRULE - Communications Server IP rules display report

The Communications Server IP rules display report describes the IP filter rule configuration of TCP/IP stacks. The field values reported can be changed through the use of IPSEC statements.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES. For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_RULE: TCP/IP Rule Configuration" on page 1073.

The batch report to review the IP rules is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP rules display report are shown in Figure 372 and Figure 373.

```
Communications Server IP rules display                          Line 1 of 2
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                  16 Aug 2010 12:53
   Complex  Sysplex  Syst     Stack    Count
   SYS1     PLEX1    IPO1     TCPIP          2
   Stack    Protoc Source IP                              SPort Destination IP
__ TCPIP                                                     0
__ TCPIP                                                     0
****************************** Bottom of Data ********************************
```

Figure 372. Communications Server IP rules overview display

```
Communications Server IP rules display                         Line 1 of 21
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                  16 Aug 2010 12:53

 IP stack data
_ Complex name                 SYS1
_ Stack name                   TCPIP
_ System SMF ID                IPO1
  Sysplex name                 PLEX1

  RULE data
  IP Protocol
  Source IP address
  Source IPv4 subnet mask
  Source port                     0
  Source IP prefix length         0
  Destination IP address
  Destination IPv4 subnet mask
  Destination port                0
  Destination IP prefix length    0
_ Routing type                 LOCAL
  Security class                 0
  Code if not all                0
```

Figure 373. Communications Server IP rules detail display

IPVIPA - Communications Server IP VIPA report

The Communications Server IP VIPA display report describes the IP Virtual IP address (VIPA) configuration of TCP/IP stacks. The field values reported can be changed through the use of VIPADYNAMIC statements.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_VIPA: TCP/IP VIPA configuration" on page 1087.

The batch report to review the IP VIPA configuration is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP VIPA display report are shown in Figure 374 and Figure 375.

```
 Communications Server IP VIPA display                Line 1 of 1
Command ===> ____________________________________________ Scroll===> CSR_
All TCP/IP stack information                    12 Oct 2009 02:19
   Complex  Sysplex  Syst     Stack    Count
   EZOS     EZOSRD2R EZOS     TCPIP          1               =
   Stack    Interface        Act VIPA                         IP ran
__ TCPIP    INTANANSE        Yes 9EEF::098E:EA40
```

Figure 374. Communications Server IP VIPA overview display

```
 Communications Server IP VIPA display              Line 1 of 16
Command ===> ____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    12 Oct 2009 02:19

 IP stack data
  Complex name                 EZOS
  Stack name                   TCPIP
  System SMF ID                EZOS
  Sysplex name                 EZOSRD2R

  VIPA data
  IPv6 interface name          INTANANSE
  Active                       Yes
  Virtual IP address           9EEF::098E:EA40
  IPv4 IP range subnet mask
  VIPA address type            Backup
  VIPA options                 MOVEABLE IMMEDIATE
  IP range prefix length       123
  VIPA Backup rank               3
```

Figure 375. Communications Server IP VIPA detail display

IPINTFD - Communications Server IP interfaces report

The Communications Server IP interfaces report describes the interface configuration of TCP/IP stacks. The field values reported can be changed through the use of DEVICE, LINK, HOME, and INTERFACE statements.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_INTERFACE: TCP/IP interface configuration" on page 1056.

The batch report to review the IP interface configuration is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP interfaces report are shown in Figure 376 and Figure 377.

```
Communications Server IP interfaces display                      Line 1 of 4
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                  16 Aug 2010 12:53
   Complex  Sysplex  Syst     Stack    Count
   SYS1     PLEX1    IPO1     TCPIP        4
   Stack    Interface        Intf type      Index
__ TCPIP    EELINK           PTP              13
__ TCPIP    LVIPA01          VIRTUAL          11
__ TCPIP    TCPIPLINK        OSAETH            9
__ TCPIP    TCPIPLINK6       PTP              15
****************************** Bottom of Data ******************************
```

Figure 376. Communications Server IP interfaces overview display

```
Communications Server IP interfaces                          Line 1 of 21
Command ===> _____________________________________________ Scroll===> CSR_
All TCP/IP stack information                 6 Aug 2009 10:03
  IP address                              IP subnet mask

  IP stack data
  Complex name                  EZOS
  Stack name                    TCPIP
  System SMF ID                 EZOS
  Sysplex name                  EZOSRD2R

  INTERFACE data
  Interface name
  Interface type                OSAETH
  Configured interface ID
  Channel path identifier       00
  IP address
  IPv4 subnet mask
  Associated name               TRLOSA26
  Source VIPA interface
  Interface options             NONE
  Security class                  0
  IP subnet addr prefix length    0
  Virtual LAN id                   0
  Virtual MAC address           000000000000
```

Figure 377. Communications Server IP interfaces detail display

IPROUTE - Communications Server IP routes report

The Communications Server IP routes report describes the route configuration of TCP/IP stacks.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES. For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_ROUTE: TCP/IP route configuration" on page 1072.

The batch report to review the IP route configuration is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP routes report are shown in Figure 378 on page 495 and Figure 379 on page 495.

```
Communications Server IP routes display                          Line 1 of 4
Command ===> _____________________________________________Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53
   Complex  Sysplex  Syst     Stack    Count
   SYS1     PLEX1    IPO1     TCPIP          4
   Stack    Destination IP                      Next hop IP address
__ TCPIP    ::                                  2002:92A:111:501:9:42:63:22
__ TCPIP    0.0.0.0                             9.42.45.1
__ TCPIP    2002:92A:111:501:9:42:63:226
__ TCPIP    9.42.45.1
****************************** Bottom of Data ********************************
```

Figure 378. Communications Server IP routes overview display

```
Communications Server IP routes display                        Line 1 of 16
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53

  IP stack data
_ Complex name                 SYS1
_ Stack name                   TCPIP
_ System SMF ID                IPO1
  Sysplex name                 PLEX1

  ROUTE data
_ Destination IP address       ::
  Next hop IP address          2002:92A:111:501:9:42:63:226
  Destination interface name   TCPIPLINK6
  Destination interface index          15
  IPv4 Destination mask
  Destination IP prefix length 0
  Static route can be replaced No
  Static route replaced        No
****************************** Bottom of Data ********************************
```

Figure 379. Communications Server IP routes detail display

IPNETACC - Communications Server IP netaccess display report

The Communications Server IP netaccess report describes the network access control configuration of TCP/IP stacks. The field values reported can be changed through the use of NETACCESS statements.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES. For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in "IP_NETACCESS: TCP/IP network access control configuration" on page 1059.

The batch report to review the IP network access control configuration is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP netaccess report are shown in Figure 380 on page 496 and Figure 381 on page 496.

```
Communications Server IP netaccess display          Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR_
All TCP/IP stack information                    12 Oct 2009 02:17
   Complex  Sysplex  Syst     Stack    Count
   EZOS     EZOSRD2R EZOS     TCPIP        3
   Stack    Resname  In  Out IP address                        IP subnet
__ TCPIP    ANANSE   Yes Yes 9.142.234.64                      255.255.25
__ TCPIP    DINO     Yes Yes 9.142.234.84                      255.255.25
__ TCPIP    FORBIDDN Yes Yes 192.168.254.254                   255.255.25
```

Figure 380. Communications Server IP netaccess overview display

```
Communications Server IP netaccess display         Line 1 of 16
Command ===> _____________________________________________ Scroll===> CSR_
All TCP/IP stack information                    12 Oct 2009 02:17

    IP stack data
  Complex name                  EZOS
  Stack name                    TCPIP
  System SMF ID                 EZOS
  Sysplex name                  EZOSRD2R

  NETACCESS data
  Last qualifier resource name  ANANSE
  Check inbound requests        Yes
  Check outbound requests       Yes
  IP address or DEFAULT(HOME)   9.142.234.64
  IPv4 subnet mask              255.255.255.224
  IP address prefix length       27
_ SERVAUTH resource name        EZB.NETACCESS.EZOS.TCPIP.ANANSE
```

Figure 381. Communications Server IP netaccess detail display

IPAUTOL - Communications Server IP autolog report

The Communications Server IP autolog report describes lists of MVS started procedures to be started by the Autolog task when TCP/IP stacks are started. The field values reported can be changed through the use of AUTOLOG statements.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option `TCPIP=YES`. For details on creating this file, see Chapter 16, “zSecure Collect for z/OS,” on page 1591.

For detailed field information, press F1 on the selection panel or any field to open the help. You can also review the field descriptions in “IP_AUTOLOG: TCP/IP autolog configuration” on page 1055.

The batch report to review the IP autolog configuration is CKALSIP. The interactive report is called CKADSIP.

Sample ISPF overview and detail displays for the Communications Server IP autolog report are shown in Figure 382 on page 497 and Figure 383 on page 497.

```
Communications Server IP autolog display                          Line 1 of 2
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53
   Complex  Sysplex  Syst     Stack    Count
   SYS1     PLEX1    IPO1     TCPIP          2
   Stack    Job Name ProcName Wa Parameter
__ TCPIP    FTPD     FTPD1     5
__ TCPIP    RXSERVE  RXSERVE   5
****************************** Bottom of Data ********************************
```

Figure 382. Communications Server IP autolog overview display

```
Communications Server IP autolog display                         Line 1 of 13
Command ===> _____________________________________________ Scroll===> PAGE
All TCP/IP stack information                    16 Aug 2010 12:53
   Stack    Job Name ProcName Wa Parameter
   TCPIP    FTPD     FTPD1     5

  IP stack data
_ Complex name                  SYS1
_ Stack name                    TCPIP
_ System SMF ID                 IPO1
  Sysplex name                  PLEX1

  AUTOLOG data
_ Job name                      FTPD
  Procedure name                FTPD1
  Max wait for restart, minutes  5
  AUTOLOG options               NONE
  Parameter string for proc.
****************************** Bottom of Data ********************************
```

Figure 383. Communications Server IP autolog detail display

IPRESOLV - Communications Server resolver report

The Communications Server IP resolver report describes the Communications Server (CS) Resolver configuration settings.

The data for this report is only available if a CKFREEZE file has been created during an APF-authorized run of zSecure Collect with option TCPIP=YES.

For details on creating this file, see Chapter 16, "zSecure Collect for z/OS," on page 1591. For detailed field information, press PF1 on the selection panel or on any field to open the help. You can also review the field descriptions in "IP_RESOLVER: CS Resolver configuration" on page 1066.

The batch report to review the IP resolver configuration is CKALSIP. The interactive report is called CKADSIP.

Figure 384 on page 498 shows a sample ISPF detail display for the Communications Server IP resolver report.

```
                                                                Line 1 of 43
Communications Server IP resolver display
Command ===> _____________________________________________ Scroll===> CSR
                                          31 Aug 2011 10:57
 System identification
  Complex name                  NMPIPL87
  System SMF ID                 IPO1
  Sysplex name                  PLEX1
  System SYSNAME                IPO1

 TCP/IP stack specifications
  Stack name
  Host name

 Resolver settings
  GLOBALTCPIPDATA specified     No        Common search order           No
  Skip unresponsive nameservers No        Unresponsive threshold (%)     25
  Cache resolved DNS queries    Yes       Cache size (MB)
  Resolve via TCP                         Name resolution order
  Always write to operator                Resolver UDP retries (max. #)
  Setup file employed           No        Resolver timeout (ms)
  Test socket storage                     Maximum time to live (s)      2147483
  Min. dots for init lkup as is
  Prefix of dynamic TCP/IP DSNs
  DBCS table names

 Resolver configuration files/data sets
  Setup file
  Default TCPIP.DATA file
  Global TCPIP.DATA file
  Default IPNODES file
  Global IPNODES file

 DNS IP addresses                       Port

 Domain origins
  Preferred network addresses   Masks

 Audit concern
  Relative audit priority        26
  Audit concern                 Any user can redirect all DNS queries from the
  Audit concern                 user's address space
****************************** Bottom of Data ********************************
```

Figure 384. Communications Server IP resolver display

Auditing the IP resolver

The following considerations apply when auditing the IP resolver.

- By default, no user should be able to redirect all DNS queries from their address spaces.
- By default, no user should be able to control CS Resolver configuration parameters. Being able to do so enables a user to redirect all IP traffic to host names from all users address spaces after the next CS Resolver setup modification.

  Even when IPRESOLV shows no concern of users being able to control CS Resolver parameters, it is possible that certain users are able to do so. To show the access of individual users to sensitive resources, examine the following reports:

  – "TRUSTUSR - Trusted users report" on page 292
  – "SENSTRUS - Sensitive Data Trustees report" on page 317

STATUS AUDIT - MVS extended tables

This section describes the z/OS system report types available in Security zSecure that require a full CKFREEZE data set read. For each report type, the background is discussed, and sample displays or batch report output are presented and discussed.

The report types described in this section are available in batch mode, and under ISPF in STATUS AUDIT category MVS extended.

Note: In general, running the latest version of zSecure Collect APF-authorized results in the most detailed reports. Running older versions of zSecure Collect as non-APF typically creates reports with missing information.

The following system reports are available:

- DMS - DMS setting report
- EXITS - Exit and table report
- DASDVOL - DASD volume report
- MOUNT - Effective UNIX mount points
- SENSITIVE - Sensitive Data Set report

DMS - DMS setting report

The DMS report describes the system's SAMS:Disk or DMS (Disk Management System) settings. A full CKFREEZE file read is required.

This report requires a CKFREEZE file. A non-authorized zSecure Collect run suffices.

The batch report to review DMS settings is CKALSDMS. The interactive report is called CKADSDMS. The language reference section for this report type is (TYPE=SYSTEM) included in Chapter 13, “SELECT/LIST Fields,” on page 953.

A sample display is included in Figure 385.

```
DMS system settings                                          Line 1 of 12
Command ===> ____________________________________________ Scroll===> CSR_
                                          10 Nov 1992 12:55
   Complex  System   Collect time stamp
   DMS00073 T#D1     10 Nov 1992 12:55

DMS options
DMS PARMLIB override restrict N
DMS 1st qual backup profiles  #GCDMS
DMS profile disk volume       GCF101
DMS call RACF non-indic       Y
DMS support for RACF          Y
DMS backup discretes          F
DMS predefined discrete OK    N
DMS process protected only    Y
DMS NEWNAME allowed           Y
DMS test DASDVOL first        N
****************************** Bottom of Data ********************************
```

Figure 385. DMS Settings display

The display contains the following fields of interest:

Table 242. DMS system settings - field descriptions

Field	Explanation
DMS PARMLIB override restrict	Indicated whether the site has restricted the use of DMS PARMLIBs to a set of specific data set names. If this option is not set, this is a major security loophole as any user can deactivate RACF processing in DMS and hence bypass RACF security.
DMS 1st qual backup profiles	The first qualifier used to backup discrete profiles.
DMS profile disk volume	The volume used to back up discrete profiles.
DMS call RACF non-indic	Indicates whether RACF is called for non-indicated data sets. Should be set (Y) on systems that have DFP.
DMS support for RACF	Indicates whether DMS supports RACF-protected data sets. If not set, DMS does not back up or restore RACF-protected data sets. If set, behavior depends on the 'process protected' setting.
DMS backup discretes	Indicates whether DMS does back up discrete profiles. Can be set to Y (save profiles for archive, but not for backup); N (save profiles for backup and archive), or F (never save profiles).
DMS predefined discrete OK	Indicates whether pre-defined discrete profiles are used on restore.
DMS process protected only	Indicates whether DMS processes RACF-protected data sets only (Y) or unprotected data sets too (N).
DMS NEWNAME allowed	Indicates whether a rename is allowed when a data set is restored. Should be set to N. If set to Y, this indicates a security exposure: DMS only checks access on the new (target) name, not the name being restored.
DMS test DASDVOL first	Indicates whether DMS is to use the RACF DASDVOL class.

The batch report is equivalent and is not shown.

Note: When precompiled DMS options are used, they might not be picked up by Security zSecure causing the program to fall back to the default settings. To avoid confusion, specify the DMS option settings in the parmlib configuration.

A second report DMSAUDIT shows the audit concerns identified.

```
DMS system settings - audit concerns                              Line 1 of 3
Command ===> ____________________________________________ Scroll===> CSR_
                                          10 Nov 1992 12:55
   Pri Complex  System   Count
    40 DMS00073 T#D1         3
   Pri Parameter               Value    Audit concern
__  40 ADSTS148                N        DMS parameter override not secured
s_  35 RACFNEWN                Y        DMS restore to newname does not check
__   1 SECURVOL                N        DMS does not use DASDVOL, this is inef
****************************** Bottom of Data ********************************
```

Figure 386. DMS Settings Audit concerns display

The display contains the following fields of interest.

Table 243. DMS Settings Audit concerns display - field descriptions

Field	Explanation
Pri	The highest priority for any DMS audit concern for this system
Complex	The complex name
System	The system name
Count	The number of DMS audit concerns for this system
Pri	A measure for the severity of the audit concern
Parameter	The SAMS:Disk parameter that causes the audit concern
Value	The value the parameter is set to
Audit concern	The audit concern identified for this setting

Select an audit concern for a detail display.

```
DMS system settings - audit concerns                          Line 1 of 13
Command ===> ____________________________________________ Scroll===> CSR_
                                          10 Nov 1992 12:55
System
Complex name                DMS00073
System name                 T#D1

DMS setting
Parameter name              RACFNEWN
Parameter value             Y

Audit concern
Relative audit priority     35
Audit concern               DMS restore to newname does not check RACF
Audit concern               authority
****************************** Bottom of Data ********************************
```

Figure 387. DMS Settings Audit concerns detail display

The detail display shows no additional information.

EXITS - Exit and table report

Security zSecure reports on the exits used by various parts of z/OS, as well as the RACF tables. This report type works 'live' (with limited functionality) or by using a CKFREEZE file.

The RACF exits and tables can be reported on a live system. ACF2, CA-1, JES2, JES3, MPF, SMF, TSO, and WTO exits as well as I/O Appendages require a CKFREEZE file. More JES exits will be shown if the CKFREEZE file was produced by an APF-authorized Collect run. Dynamic exits require an APF-authorized run unless specific permits were given. HSM and SAMS:Disk (DMS) exits require an APF-authorized run.

Background

Exits are installation-defined programs that are called at well-defined points by MVS, system programs such as JES2 or RACF and ACF2, or third-party programs, in order to assist or alter the decision-making process of the calling program. An example of this is the RACF password encryption exit, ICHDEX01, which decides the type of password encryption to be used, and can even be used by an installation to implement a local encryption method.

Exits often execute in *key 0* which might grant the authority to alter MVS access control decisions.

Auditors should always review which exits are active; exits can be used to alter system security without changing the system's code or its visible parameters. Source code should be reviewed for all installation-written exits, and all changes should be monitored.

Auditing exits

Security zSecure can assist in auditing exits by showing the active exits and their contents. The following exit information can be audited:

- RACF and ACF2 exits
- SMF, TSO, JES2, JES3, DMS, HSM, MPF, WTO, and CA-1 exits.
- I/O appendages.
- Exits from the MVS 5.1 dynamic exit facility.

The input is taken from the actual in-storage control blocks that define whether an exit is used or not. For SMF exits, the decision whether an exit is taken or not can be defined separately for each subsystem. The SMF subsystem-dependent information is reported by another report type, see "SMFSUBOP - SMF subsystem report" on page 446. Exits IEFUSO and IEFUJP can even be activated on the job-class level in JES2. This is reported in the JES2 job-class report, see "JOBCLASS - JES2 Job Class report" on page 460.

The information displayed includes the *entry point* address, the *virtual storage area* where the entry point resides, and the leading 256 bytes of the exit, usually containing an eye catcher with a level indicator or copyright notice. In addition, an automatic *disassembly* is performed to see whether the exit returns a fixed return code 0, 4, or 8. The results of an instruction, string, and SVC scan performed by zSecure Collect are also shown.

The batch report to review the exits is CKALSXIT. The interactive report is called CKADSXIT.

Sample ISPF overview and detail displays for the exit report are shown in Figure 388 on page 503 and Figure 389 on page 504.

```
Exit and table overview                                        Line 1 of 35
Command ===> ____________________________________________ Scroll===> CSR_
                                          30 Mar 2004 00:07
    Complex  System   Exits Audit concerns Priority
    SYS1     IPO1       126              1        5
    Pri Program  Applic   Subs Dynamic exitname Eff Description
__    5 CNZM1SSX dynamic       IEASDUMP.SERVER  Yes SVC dump exit for adding dat
__      ADYHCADC dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      ARCHCEXT dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      BLWHCADC dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      BPXHCADC dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      CBRHADUX OAM                                Object access method auto-de
__      CBRUXCUA OAM                                Object access method change
__      CBRUXEJC OAM                                Object access method cartrid
__      CBRUXENT OAM                                Object access method cartrid
__      CBRUXSAE OAM                                Object access method authori
__      CBRUXVNL OAM                                Object access method volume
__      CEAMDMPX dynamic       IEASDUMP.SERVER  Yes SVC dump exit for adding dat
__      CEAPSNPX dynamic       IEASDUMP.POSTDMP Yes
__      CELSDLPA dynamic       CSVDYLPA         Yes Dynamic LPA notification mec
__      CELSHADD dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      CNZHCADC dynamic       HZSADDCHECK      Yes Health Checker for z/OS
__      CNZM1DYX dynamic       CSVDYNEX         Yes Dynamic exit facility
__      CSFHCADD dynamic       HZSADDCHECK      Yes Health Checker for z/OS
****************************** Bottom of Data ********************************
```

Figure 388. Exit Overview display

The overview display contains the following fields of interest.

Table 244. Exit and table overview - field descriptions

Field	Explanation
Complex	Name of the complex examined.
System	Name of the system examined.
Exits	The number of exits analyzed for the system.
Audit concerns	The number of exits for which audit concerns were identified.
Priority	The highest numerical audit priority identified.
Pri	Numerical audit priority assigned to the exit.
Program	The documented name of the exit (does not need to correspond to the actual module name).
Applic	The application owning the exit.
Subs	The subsystem name, if the application is JES2.
Dynamic exitname	The full name of the exit point, if the exit is dynamic.
Eff	Indicates if the module is called as a dynamic exit routine.
Description	A description of the function of the exit.
Means	The result from an automatic disassembly of the exit code.
Address	Address of the exit or table.
Where	Exit residency.
Key SP	The key and sub-pool of the storage area where the exit is located.
Jobname	The jobname of the address space owning the exit, if the exit resides in private storage.
Length	Approximate length of the exit module.
Exit at	Exit program name, module name and offset
InstrScan	Results of an instruction scan performed by zSecure Collect.

Table 244. Exit and table overview - field descriptions (continued)

Field	Explanation
Str	Results of a string scan performed by zSecure Collect.
Eye catchers	Start of the exit or table (nonprintables have been replaced by dots).
Audit concern	Audit concerns identified.

Select any of these for a detailed view of the exit, showing the location of the exits, the eye catchers in the first 256 bytes of the exit, and an interpretation of the exit based on a simple disassembly of the instructions.

```
Exit and table overview                                          Line 1 of 31
Command ===> _____________________________________________ Scroll===> PAGE
                                          8 Sep 2009 13:30
   Complex  System   Exits Audit concerns Priority
   SYS1     ACF2        68              1        5
   Pri Program  Applic   Subs Dynamic exitname Eff Description
     5 CNZM1SSX dynamic       IEASDUMP.SERVER  Yes SVC dump exit for adding dat
Address  Where   Key SP  Jobname       Length AM Exit at
02977AB0 EPLPA                          57576 31 CNZM1SSX in CNZINLPA
Appl     Subs Dynamic exitname Description
dynamic       IEASDUMP.SERVER  SVC dump exit for adding data to the dump
Act Def Eff FiltType JobFilt  Stoken filter
Yes Yes Yes
Any ExK Pos Param
No    0 149
InstrScan Str SVC scan result
ModeSupRB  No
Eye catchers
..CNZM1SSX02/16/06 HBB7730.\{{..-}m..}qo..S k..

Audit concern
Instruction scan hit
First 256 bytes of exit
0000. A7F40010 00000000 C3D5E9D4 F1E2E2E7 *x4......CNZM1SSX*
****************************** Bottom of Data ********************************
```

Figure 389. Exit detail display

The detail display contains the following fields of interest:

Table 245. Exit and Table overview - field descriptions

Field	Explanation
Address	The address of the exit.
Where	Exit residency.
Key SP	the key and sub-pool of the storage area where the exit is located.
Jobname	The jobname of the address space owning the exit, if the exit resides in private storage.
Length	Approximate length of the exit module.
AM	Addressing mode.
Exit at	Module information and offset for the exit.
Appl	The application owning the exit.
Subs	The subsystem name, if the application is JES2.
Exitname	The full name of the exit point, if the exit is dynamic.
Description	The documented function of the exit.

Table 245. Exit and Table overview - field descriptions (continued)

Field	Explanation
Act	Indicates if a module is active.
Def	Indicates if the module has been added to a defined exit point.
Eff	Indicates if the module is called as a dynamic exit routine.
FiltTyp	Indicates the type of filter defined for the exit module.
JobFilt	The JOB filter pattern used to control if this module is called.
Stoken filter	The Address Space STOKEN used to control if this module is called.
InstrScan	Results of an instruction scan performed by zSecure Collect.
Str	Results of a string scan performed by zSecure Collect.
SVC scan result	Results of an SVC scan performed by zSecure Collect.
Eye catchers	Contents of the exit; non-printable characters have been replaced by periods.
Result	Result of disassembly. RC=*x* indicates the exit has a fixed return code *x*.
Audit concern	Audit concerns identified.
First 256 bytes of exit	The start of the exit is shown both in hex and text. Nonprintables have been replaced with periods in the latter.

A sample batch report is shown in Figure 390 on page 506.

```
E X I T   O V E R V I E W   26 Sep 2002 00:07
Exit and table overview


Complex  System   Exits Audit concerns Priority
C#M4     C#M4        21              0

Pri Appl     Subs Exit     Address  Jobname  Where   Key SP  Length AM Entry at
                           Dynamic exitname  Eff Description
                           Result / Audit concern

    dynamic       IEFACTRT 084A1000          EMLPA             2128 31 IEFACTRT
                           SYS.IEFACTRT      Yes SMF job/step termination exit

    dynamic       IEFDB401 0410EB40          EPLPA               32 31 IEFDB401
                           IEFDB401          Yes Dynamic allocation validation routi
                           RC=0
    dynamic       IEFUAV   023AF420          EPLPA               32 31 IEFUAV
                           SYS.IEFUAV        Yes User account validation exit for AP
                           RC=0
    dynamic       IEFUJI   024D2B98          EPLPA               32 31 IEFUJI
                           SYS.IEFUJI        Yes Job initiation exit
                           RC=0
    dynamic       IEFUJP   0531D798          EPLPA               32 31 IEFUJP
                           SYS.IEFUJP        Yes Job purge exit
                           RC=0
    dynamic       IEFUJV   03AB86F8          EPLPA               32 31 IEFUJV
                           SYS.IEFUJV        Yes Job validation exit (JCL conversion
                           RC=0
    dynamic       IEFUSI   023AA728          EPLPA               32 31 IEFUSI
                           SYS.IEFUSI        Yes Step initiation exit
                           RC=0
    dynamic       IEFUSO   050DC5F0          EPLPA               32 31 IEFUSO
                           SYS.IEFUSO        Yes Sysout limit exit
                           RC=0
    dynamic       IEFUTL   070FB498          EPLPA               32 31 IEFUTL
                           SYS.IEFUTL        Yes Time limit exit
                           RC=0
    dynamic       IEFU29   03AE3588          EPLPA               32 31 IEFU29
                           SYS.IEFU29        Yes SMF dataset switch ("dump") exit
                           RC=0
    dynamic       IEFU83   0557B3E0          EPLPA               32 31 IEFU83
                           SYS.IEFU83        Yes SMF record exit SVC-entry SMFWTM
                           RC=0
    dynamic       IEFU84   039C9288          EPLPA               32 31 IEFU84
                           SYS.IEFU84        Yes SMF record exit branch-entry SMFWTM
                           RC=0
    dynamic       IEFU85   023A8FE0          EPLPA               32 31 IEFU85
                           SYS.IEFU85        Yes SMF record exit cross-memory SMFWTM
                           RC=0

    IOAPP         IGG019E4 00000000          PSA                   24
                                             Yes Authorized I/O appendage

    JES2     JES2 HASX5CTR 0A522348 JES2     EPVT                  31
                                             Yes JES2 Command Preprocessor
```

Figure 390. Batch Exit Report - page 1

```
E X I T   O V E R V I E W   26 Sep 2002 00:07
Exit and table overview

    MPF           DSNWAIT  090CE000          ECSA     0 241    4096 31

    MPF           WTOREPLY 0924EE88          ECSA     0 241     376 31

    MVS           IEFDOIXT 00000000          PSA                    24
                                             Edit/check OUTADD/OUTDEL parameters

    RACF          ICHAUTAB 00E15CE8          PLPA                88 24 ICHAUTAB
                                             Authorized caller table

    RACF          ICHRCX02 084A2F88          EMLPA             2160 31 ICHRCX02
                                             RACHECK postprocessing exit

    TSO           IKJEFF10 00000000          PSA                    24
                                             SUBMIT command exit
```

Figure 391. Batch Exit Report - page 2

In addition, the Dynamic exit definitions are shown. Figure 392 shows the overview display for this report. Additional fields are shown when you scroll right on the display. See Figure 393 on page 508.

```
Dynamic exit definitions                                      Line 1 of 73
Command ===> _____________________________________________ Scroll===> PAGE
                                          29 Jun 2010 09:12
   Complex  System   Exits
   SYS1     IPO1        73
   Dynamic exitname Description                                Exp #Acti #In
__ BPX_IMAGE_INIT   UNIX process image initiation exit         Yes     0
__ BPX_POSPROC_INIT UNIX post-process initiation exit          Yes     0
__ BPX_PREPROC_INIT UNIX pre-process initiation exit           Yes     1
__ BPX_PREPROC_TERM UNIX pre-process termination exit          Yes     0
__ CEE_ABEND_EXIT                                             Yes     0
__ CNZ_MSGTOSYSLOG  Message to Syslog exit                     Yes     0
__ CNZ_WTOMDBEXIT   WTO Message Data Block exit                Yes     0
__ CSVDYLPA         Dynamic LPA notification mechanism         Yes     4
__ CSVDYNEX         Dynamic exit facility                      Yes     3
__ CSVLLIX1         LLA module fetch exit                      Yes     1
__ CSVLLIX2         LLA module staging exit                    Yes     1
__ C2X.ICHPWX01     New password exit                          Yes     0
__ C2X.ICHPWX01.PRE New password exit                          Yes     0
__ C2X.ICHPWX01.PST New password exit                          Yes     1
__ C2X.ICHRCX02     RACHECK postprocessing exit                Yes     0
__ C2X.ICHRCX02.PRE RACHECK postprocessing exit                Yes     0
__ C2X.ICHRCX02.PST RACHECK postprocessing exit                Yes     1
__ C2X.ICHRDX02     RACDEF postprocessing exit                 Yes     0
```

Figure 392. Dynamic exit definitions - Overview display panel (first screen)

```
Dynamic exit definitions                                      Line 37 of 73
Command ===> _____________________________________________ Scroll===> PAGE
                                          29 Jun 2010 09:12
   Complex  System   Exits
   SYS1     IPO1        73
                          Exp #Acti #Inac Amo #Abnd CAb Fst Any ExK Ren Sgl
__  wait exit              Yes     0     0 31  ***** No  No        0 Yes No
__                         Yes     0     0 31  ***** No  No        0 Yes No
__                         Yes     0     0 31  ***** No  No        0 Yes No
__ validation routine      Yes     1     0 Def ***** No  Yes       1 Yes No
__                         Yes     0     0 31  ***** No  Yes Yes   0 Yes No
__                         Yes     0     0 31      1 No  No        5 No  No
__                         Yes     1     0 31  ***** No  No        0 Yes No
__  Exit                   Yes     0     0 31  ***** Yes Yes       0 Yes No
__ alidation Exit          Yes     0     0 31  ***** Yes No        0 Yes No
__ on scope=systems notify Yes     0     0 31      1 No  Yes       0 Yes No
__ on scope=system notify  Yes     0     0 31      1 No  Yes       0 Yes No
__ e exit                  Yes     2     0 31      1 No  Yes       0 Yes No
__ l DEQ exit              Yes     0     0 31      1 No  Yes       0 Yes No
__ t                       Yes     0     0 31      1 No  Yes       0 Yes No
__ ched exit               Yes     0     0 31      1 No  Yes       0 Yes No
__ ditional batch exit     Yes     0     0 31      1 No  Yes       0 Yes No
__ E exit                  Yes     0     0 31      1 No  Yes       0 Yes No
__ ch pre-processing exit  Yes     0     0 31      1 No  Yes       0 Yes No
```

Figure 393. Dynamic Exit Definitions Overview display panel (scroll right)

Table 246 lists the fields on interest on the Dynamic exit definitions overview report shown in Figure 392 on page 507 and Figure 393.

Table 246. Dynamic Exit Definitions - Overview field descriptions

Field	Description
Description	String explaining the function of the exit.
Dynamic exit name	Full name of the dynamic exit.
Exp	Indicates if the exit point module has been defined.
#Acti	Number of active exit routines for the exit point.
#Inac	Number of added, but inactive exit routines for exit point.
Amo	The required addressing mode for exit routines.
#Abnd	Number of abnormal endings an exit routine can have.
CAb	Indicates if the total number of abnormal endings for the exit routines is counted consecutively or cumulatively.
Fst	Indicates if the exit routine can be called in fast path mode.
Any	Indicates if the exit routine can be called in any key.
ExK	The storage key and execution key.
Ren	Indicates if the exit routine is required to be reentrant.
Sgl	Indicates if the exit can have only a single module associated with it at a given point in time.

To view detailed information for any of the exits included in the Dynamic definition overview display panel, type the **S** in the selection field for the report to open the detail display shown in Figure 394 on page 509..

```
Dynamic exit definitions                                        Line 1 of 14
Command ===> _____________________________________________ Scroll===> PAGE
                                          29 Jun 2010 09:12
   Complex  System   Exits
   SYS1     IPO1        73
                           Exp #Acti #Inac Amo #Abnd CAb Fst Any ExK Ren Sgl
   initiation exit         Yes     0     0 31  10000 Yes Yes       0 Yes No

Exit point defined         Yes
Number of active routines      0
Number of inactive routines    0

Addressing mode            31
Fastpath call enabled      Yes
Abends before deactivate   10000
Fast path uses any key
Abend count is consecutive Yes
Execution key                0

Only one routine for exit  No
Exit routine must be rent  Yes
****************************** Bottom of Data ********************************
```

Figure 394. Dynamic exit definitions - Detail display panel

DASDVOL - DASD volume report

Security zSecure allows you to view the Direct Access Storage Device (DASD) volumes connected to up to 32 systems; a CKFREEZE file for each of these systems is required. The report generated provides an overview of each of the DASD volumes on-line on at least one system; it can be edited to include all DASD volumes that are not on-line, but are referred to (e.g. in ICF catalogs).

This report requires a CKFREEZE file. A non-authorized zSecure Collect run suffices.

Note: unlike the other reports, which focus on resources or tables *per system*, the DASD volume report focuses on volumes, and shows the systems only relative to the DASD volumes connected.

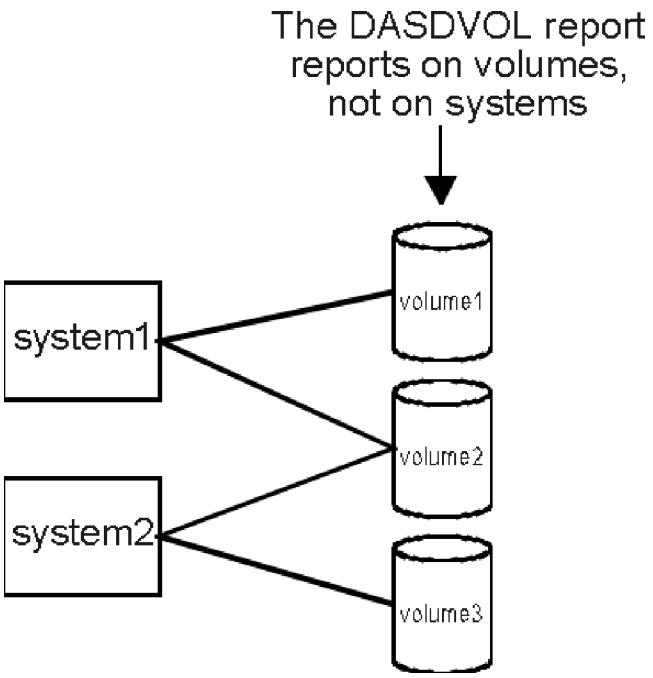


Figure 395. DASD Volumes

Background

DASD volumes can be accessed by one or more systems. This sharing is done by channels that connect systems to the control unit controlling the device where the volume is mounted.

Depending on the site, device numbers might or might not be the same across systems. Also, two systems showing a volume mounted with the same volume serial, do not need to share the same physical volume, even when the device numbers are the same. The former often happens if a site connects (merges) two different systems, the latter often happens if the site employs 'string switching' as a means to control change. For example, a complete DASD string is first used non-shared on a test system and is then connected to the production system. This separates test and production very well and leaves volume serials the same.

The DASD box serial number can be used to determine the sharing properties quite easily - but only more recent device types support this.

The values shown in the DASDVOL report are specified in parmlib member VATLSTxx, in the SMS control data set, the HCD, the MVSCP, and the IOGEN.

Auditing DASD Volumes

For Security zSecure to report on exposures reliably, it should know how volumes are shared across systems. The protection of the same data set can be different on different systems.

It is also checked that if two systems share the same volume, the volume is known to MVS as shared. If it is not, serialization (reserve and release processing) is not done when updating the volume, which can result in an undefined state of the volume when the two systems perform an update simultaneously.

The SMS management of DASD volumes is of importance too; data sets in the APF list that are specified without VolSer are only APF if they reside on an SMS managed volume.

The batch report to review DASD volumes is CKALVOLD. The interactive report is called CKADVOLD.

Figure 396 shows the DASD Volume overview display.

```
DASD Volume Protection and Sharing                              Line 1 of 48
Command ===> ____________________________________________ Scroll===> CSR_
                                                25 Feb 1998 18:02
  Pri VolSer Man Fa Serial       Id   Box type   # STO PUB Audit concern
s_ 40 SME000 IBM-51-000000068569-090E   IDSK-001 2         Mounted on more sys
__ 40 SME001 IBM-51-000000068569-0908   IDSK-001 2         Mounted on more sys
__ 40 SME002 IBM-51-000000068569-0909   IDSK-001 2         Mounted on more sys
__ 40 SME003 IBM-51-000000068569-090A   IDSK-001 2         Mounted on more sys
__ 40 SME004 IBM-51-000000068569-090B   IDSK-001 2         Mounted on more sys
__ 40 SME005 IBM-51-000000068569-090C   IDSK-001 2         Mounted on more sys
__ 40 SME006 IBM-51-000000068569-090D   IDSK-001 2         Mounted on more sys
__ 40 SME007 IBM-51-000000068569-0A10   IDSK-001 2         Mounted on more sys
__ 40 SME008 IBM-51-000000068569-0A11   IDSK-001 2         Mounted on more sys
__ 40 SME009 IBM-51-000000068569-0A12   IDSK-001 2         Mounted on more sys
__ 40 SME010 IBM-51-000000068569-0A13   IDSK-001 2         Mounted on more sys
__ 40 SME011 IBM-51-000000068569-0A14   IDSK-001 2         Mounted on more sys
__ 40 SME012 IBM-51-000000068569-0A15   IDSK-001 2         Mounted on more sys
__ 40 SME013 IBM-51-000000068569-0C22   IDSK-001 2         Mounted on more sys
__ 40 SME014 IBM-51-000000068569-0C23   IDSK-001 2         Mounted on more sys
__ 40 SMK001 IBM-51-000000068569-0C20   IDSK-001 2         Mounted on more sys
__ 40 SMK002 IBM-51-000000068569-0C21   IDSK-001 2         Mounted on more sys
__ 40 SYSP01 IBM-51-000000068569-0D2A   IDSK-001 2         Mounted on more sys
__ 20 DBASP4 IBM-51-000100068569-0801   IDSK-001 2         Mounted on more sys
__ 20 D1ASP4 IBM-51-000100068569-0800   IDSK-001 2         Mounted on more sys
__ 20 D2ASP4 IBM-51-000100068569-0908   IDSK-001 2         Mounted on more sys
__ 20 HFS001 IBM-51-000100068569-0B1A   IDSK-001 2         Mounted on more sys
__ 20 IPL130 IBM-51-000100068569-0A11   IDSK-001 2 YES     Mounted on more sys
__ 20 PRIM14 IBM-51-000100068569-0B18   IDSK-001 2         Mounted on more sys
__ 20 RES306 IBM-51-000000068569-0806   IDSK-001 2         Mounted on more sys
__ 20 RES31C IBM-51-000000068569-0B1C   IDSK-001 2         Mounted on more sys
__ 20 RES324 IBM-51-000000068569-0C24   IDSK-001 2         Mounted on more sys
__ 20 RES61B IBM-51-000100068569-0B1B   IDSK-001 2     YES Mounted on more sys
__ 20 RES619 IBM-51-000100068569-0B19   IDSK-001 2     YES Mounted on more sys
__ 20 R1ASP4 IBM-51-000000068569-0D28   IDSK-001 2         Mounted on more sys
__ 20 R2ASP4 IBM-51-000000068569-0D29   IDSK-001 2 YES     Mounted on more sys
__ 20 SYSJ00 IBM-51-000100068569-0909   IDSK-001 2         Mounted on more sys
__ 20 SYSP99 IBM-51-000100068569-0A12   IDSK-001 2         Mounted on more sys
__ 20 SYS100 IBM-51-000000068569-0D2B   IDSK-001 2         Mounted on more sys
__ 20 SYS101 IBM-51-000100068569-090B   IDSK-001 2         Mounted on more sys
__ 20 SYS102 IBM-51-000100068569-0A13   IDSK-001 2         Mounted on more sys
__ 20 WORKPK IBM-51-000000068569-0A16   IDSK-001 2 YES     Mounted on more sys
__    MIG000 IBM-51-000100068569-0802   IDSK-001 1
__    MIG001 IBM-51-000000068569-0800   IDSK-001 1
__    MIG002 IBM-51-000000068569-0801   IDSK-001 1
__    MIG003 IBM-51-000000068569-0802   IDSK-001 1
__    MIG004 IBM-51-000000068569-0803   IDSK-001 1
__    MIG005 IBM-51-000000068569-0804   IDSK-001 1
__    MIG007 IBM-51-000000068569-0B18   IDSK-001 1
__    MIG008 IBM-51-000000068569-0805   IDSK-001 1
__    MIG009 IBM-51-000000068569-0B19   IDSK-001 1
__    MIG010 IBM-51-000000068569-0B1A   IDSK-001 1
__    MIG011 IBM-51-000000068569-0B1B   IDSK-001 1
```

Figure 396. DASD Volume Report

The display contains the following fields of interest:

Table 247. DASD Volume Protection and Sharing - field descriptions

Field	Explanation
Pri	Relative audit priority.
VolSer	The volume serial of the DASD volume.
Man Fa Serial Id	The serial code of the volume, containing the code of the manufacturer, factory code, box serial number, and device tag.
Box type	The type of DASD volume, e.g. 3390-A28.
#	The number of systems on which the volume is mounted.
STO	Indicates whether the disk has the STORAGE mount-use attribute on any system.
PUB	Indicates whether the disk has the PUBLIC mount-use attribute on any system.
Audit concern	Audit concerns identified.

Figure 397 shows the DASD Volume detail display.

```
DASD Volume Protection and Sharing                              Line 1 of 5
Command ===> ____________________________________________ Scroll===> CSR_
                                          25 Feb 1998 18:02
   Pri VolSer Man Fa Serial       Id   Box type   # STO PUB Audit concern
    40 SME000 IBM-51-000000068569-090E   IDSK-001 2         Mounted on more sys
System   Devn Attributes    Shr Mnt SMS Use     Unit
OR37      30E               No  Yes No  PRIVATE 3380
DINO      30E               No  Yes Yes PRIVATE 3380
Audit concern
Mounted on more systems but not shared, Inconsistently SMS-managed
****************************** Bottom of Data ******************************
```

Figure 397. DASD Volume detail display.

Table 248. DASD Volume Protection and Sharing display - field descriptions

Field	Explanation
System	The name of a system to which the volume is connected. On the rest of the line, all fields following the system name, except for the audit concern, apply to that system only.
Devn	The device number of the DASD volume on the current system.
Attributes	Attributes for the volume on this system. This field can contain one or more of the following values: *IPL* (IPL volume) *MCAT* (contains the master catalog) *PAGE* (contains a page data set)
Shr	Indicates whether the system uses the DASD volume as a shared volume or not.
Mnt	Indicates whether the volume is mounted on the system.
SMS	Indicates whether the volume is SMS-managed on the system.
Use	The mount-use attribute of the volume; can be PRIVATE, PUBLIC, and STORAGE.
Unit	The unit type of the volume.

MOUNT - Effective UNIX mount points

The MOUNT report shows the effective UNIX mount points. A full CKFREEZE read is required, and the CKFREEZE must have been made with the UNIX=Y parameter.

This report requires a CKFREEZE file and shows more information if the zSecure Collect run was APF-authorized.

Background

z/OS UNIX files are physically contained in an hierarchical file system (HFS) or zSeries file system (zFS) data sets. A UNIX file system consists of a directory tree in which files are located. A file system is made accessible by mounting it, for example, by assigning it a position in the existing directory tree (mounting it over that directory--this hides the previous contents of that subtree). The root directory of the file system is then located at the mount point, and its subdirectories form the new subtree.

A device number is associated with each mount point (mounted file system). Together with the *inode* number which identifies a file within a file system this yields a key to a file. Starting with OS/390® Version 2 Release 9, it is possible to share file systems across a sysplex. In that case the file system is owned by one system, and others can talk to it via the Coupling Facility. Access to the DASD the file system resides on is not needed by the other systems, they refer to a specific device number.

An automount point is a special mount point where user file systems get dynamically mounted when a reference is made to a file in them. They can also be dynamically unmounted when no references are made for some amount of time.

This information can be obtained with the OMVS command **df** or the D OMVS,F operator command.

Auditing UNIX mounts

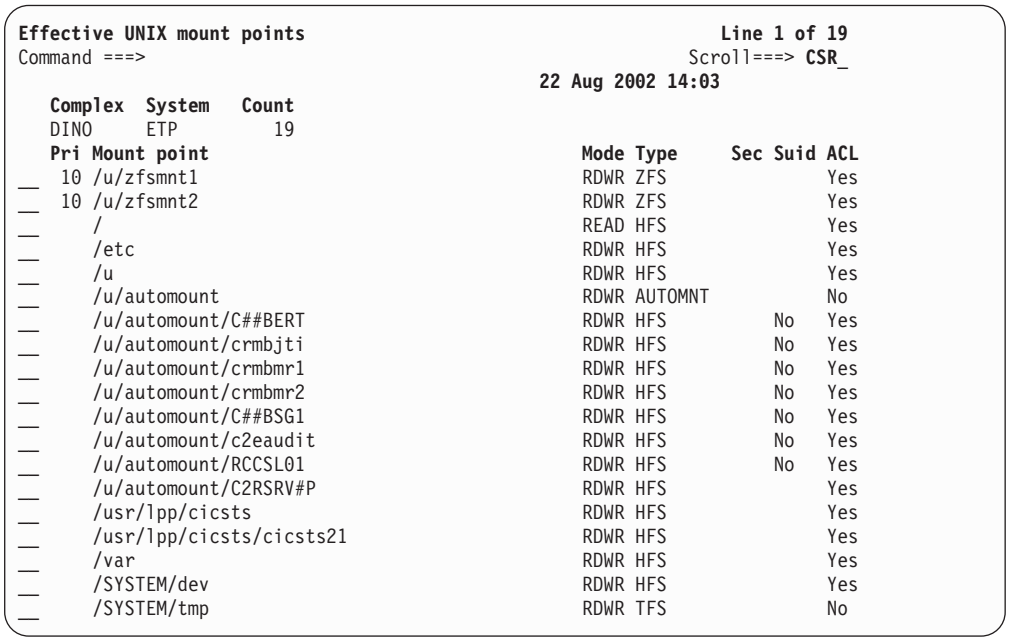
There are several mount options that are relevant for security. For instance, a file system can be mounted in such a way that the UNIX security settings are used for protection, or that they are ignored. Also the **setuid** bits can be ignored, for example, the program runs under the users own uid instead of under the program file owner's uid. A file system can also be mounted in read-only mode.

A file system might or might not support ACLs, or it might not know about ACLs. In a sysplex environment with some systems that support ACLs and some that do not, files with ACLs are inaccessible (except perhaps for the file owner or a superuser) from the downlevel systems (if they know of ACLs) if the FSSEC class is active on an up-level one.

zFS file systems have an additional NBS (New Block Security) option for clearing new blocks before they are linked to a file. This option is more or less the opposite of the EOS (Erase On Scratch) option that clears blocks when they are freed. The NBS option ensures that blocks that contain data from previous files they belonged to cannot be read if the system crashes between the moment the block is linked to a file and the moment the block is written. For security, the NBS option must be enabled to prevent someone from accessing parts of protected data. If the option is not enabled, an audit concern is issued.

The batch report to audit UNIX mount points is CKALSMNT. The interactive report is called CKADSMNT.

UNIX mount points are shown in the following figure.



```
Effective UNIX mount points                                    Line 1 of 19
Command ===>                                                 Scroll===> CSR_
                                                      22 Aug 2002 14:03
   Complex  System   Count
   DINO     ETP         19
   Pri Mount point                                  Mode Type     Sec Suid ACL
__  10 /u/zfsmnt1                                   RDWR ZFS                Yes
__  10 /u/zfsmnt2                                   RDWR ZFS                Yes
__     /                                            READ HFS                Yes
__     /etc                                         RDWR HFS                Yes
__     /u                                           RDWR HFS                Yes
__     /u/automount                                 RDWR AUTOMNT            No
__     /u/automount/C##BERT                         RDWR HFS           No   Yes
__     /u/automount/crmbjti                         RDWR HFS           No   Yes
__     /u/automount/crmbmr1                         RDWR HFS           No   Yes
__     /u/automount/crmbmr2                         RDWR HFS           No   Yes
__     /u/automount/C##BSG1                         RDWR HFS           No   Yes
__     /u/automount/c2eaudit                        RDWR HFS           No   Yes
__     /u/automount/RCCSL01                         RDWR HFS           No   Yes
__     /u/automount/C2RSRV#P                        RDWR HFS                Yes
__     /usr/lpp/cicsts                              RDWR HFS                Yes
__     /usr/lpp/cicsts/cicsts21                     RDWR HFS                Yes
__     /var                                         RDWR HFS                Yes
__     /SYSTEM/dev                                  RDWR HFS                Yes
__     /SYSTEM/tmp                                  RDWR TFS                No
__
```

The preceding figure contains the following fields of interest.

Table 249. Effective UNIX mount points - field descriptions

Field	Explanation
Audit concern	**Audit concerns identified**
Complex	The complex name.
System	The system name.
Count	The number of mount points.
Pri	Relative audit priority.
Mount point	The absolute pathname of the mount point.
Mode	The mode in which the file system is mounted: READ (read-only) or RDWR (read/write).

Table 249. Effective UNIX mount points - field descriptions (continued)

Field	Explanation
Audit concern	**Audit concerns identified**
Type	The file system type which can be any of the following: **ZFS** zSeries file system (based on DCE LFS Episode file system). **AUTOMNT** Automount point for dynamical file system mounts/unmounts **CINET** File system that handles requests for AF_INET sockets. **DFSC** Distributed global file system (under DCE). **HFS** Hierarchical (local) file system. **INET** Like CINET but assumes SecureWay Communications Server. **NFS** Network (remote) file system. **TFS** Temporary file system. **UDS** File system that handles requests for AF_UNIX sockets.
Sec	Whether the file system is mounted with the SECURITY attribute. If not, any user can access and change any file in it.
Suid	Whether the file system is mounted with the SETUID attribute. Setuid, setgid, APF, and program control attributes for files are only honored if this is the case.
ACL	Whether the file system supports Access Lists.
NBS	New Block Security. This option only applies to zFS file systems. When enabled, disk blocks are physically cleared before they are linked to a file.
RO_Secl	The assumed, read-only security label. See also “READONLY_SECLABEL” on page 1106.
File system name	The name of the file system.
Dataset	The name of the MVS data set that contains the file system.
OwnCompl	The complex the system that owns the file system mounted is in.
OwnSyst	The system that owns the file system mounted.
Device	The UNIX device number for the mounted file system.
Volser	The volume serial of the MVS data set with the file system.
RWS	A flag field that indicates whether the file system is sysplex-aware. If True, the file system was mounted with sysplex_mode=on or with PARM(RWSHARE).

Table 249. Effective UNIX mount points - field descriptions (continued)

Field	Explanation
Audit concern	**Audit concerns identified**
Plex mode	A field that indicates the zFS sysplex status. The possible values are: • **Noshare**: zFS is not in a shared file system environment. • **Admin-only**: zFS is in a shared file system environment but is not sysplex-aware. • **On**: zFS is in a sysplex-aware environment with sysplex=on. • **Filesys**: zFS is in a sysplex-aware environment with sysplex=filesys.

Select any row for a detail view of a particular mount point.

```
Effective UNIX mount points                                    Line 1 of 26
 Command ===> ____________________________________________ Scroll===> CSR_
                                          22 Aug 2002 14:03

 Viewpoint characteristics
 Complex name                  DINO
 System name                   ETP
 Mount point                   /u/zfsmnt1
 UNIX device number            14
 File system mode              RDWR
 File system type              ZFS
 File system name              ZFS.F1
 Mounted with SECURITY         Yes
 Mounted with SETUID           Yes
 File system supports ACLs     Yes
 New block security            No
 Read-only security label
 Read/Write share              No
 Sysplex mode                  Filesys
 Relative audit priority       10
 Audit concern                 Disk scavenging threat / not C2 compliant

 Physical characteristics
 Complex that owns file system DINO
 System that owns file system  ETP
 Data set name                 ETP.ZFS.FILESYS
 Volume serial                 ETPSMS
 DASD box serial number and id IBM-51-0000000113FF-0052
 Size of block in bytes        8192
 Size of fragment in bytes     1024
 Size of aggregate in blocks   2592
 ******************************* Bottom of Data ********************************
```

The detail display contains the following fields of interest:

Table 250. Effective UNIX mount points - field descriptions

Field	Explanation
Complex name	The name of the complex.
System name	The system name.
Mount point	The absolute pathname of the mount point.
UNIX device number	The UNIX device number for the mounted file system.
File system mode	The mode in which the file system is mounted: READ (read-only) or RDWR (read/write).

Table 250. Effective UNIX mount points - field descriptions (continued)

Field	Explanation
File system type	The type of file system mounted.
File system name	The name of the file system (for HFS equal to data set name)
Mounted with SECURITY	Whether the file system is mounted with the SECURITY attribute. If not, any user can access and change any file in it.
Mounted with SETUID	Whether the file system is mounted with the SETUID attribute. Setuid, setgid, APF and program control attributes for files are only honored if this is the case.
File system supports ACLs	Whether the file system supports Access Lists.
New Block Security	This option only applies to zFS file systems. When switched on, disk blocks are physically cleared before they are linked to a file.
Read-only security label	The assumed, read-only security label. See also "READONLY_SECLABEL" on page 1106.
Read/Write share	A flag field that indicates whether the file system is sysplex-aware. If True, the file system was mounted with sysplex_mode=on or with PARM(RWSHARE).
Sysplex mode	A field that indicates the zFS sysplex status. The possible values are: • **Noshare**: zFS is not in a shared file system environment. • **Admin-only**: zFS is in a shared file system environment but is not sysplex-aware. • **On**: zFS is in a sysplex-aware environment with sysplex=on. • **Filesys**: zFS is in a sysplex-aware environment with sysplex=filesys.
Relative audit priority	Relative audit priority.
Audit concern	Audit concern identified.
Complex that owns file system	The complex that owns the system that the file system is mounted in.
System that owns file system	The system that owns the file system mounted.
Data set name	The name of the MVS data set that contains the file system.
Volume serial	The volume serial of the MVS data set with the file system.
DASD box serial number and ID	The serial number of the volume containing the manufacturer, factory code, box serial number and device tag.
Size of block in bytes	Size of a block of the zFS file system in bytes (normally 8192).
Size of fragment in bytes	Size of a fragment of the zFS file system in bytes. Multiple files can share a logical block if they are smaller than (block size - fragment size). (1k,2k ... up to block size).

Table 250. Effective UNIX mount points - field descriptions (continued)

Field	Explanation
Size of aggregate in blocks	The size in blocks of the aggregate. Normally the number of blocks that fit in the primary allocation.

For a thorough look at UNIX file protection look at the following reports: "APFPROT - Authorized Programs reports" on page 328, "GLBW - Globally writable data reports" on page 348.

SENSITIVE - Sensitive Data Set report

The sensitive data set report describes the system sensitive data sets for each system.

This report requires a CKFREEZE file and shows more information if the zSecure Collect run was APF-authorized.

The sensitive data set reports list data sets on the system that are considered sensitive and pose a threat if they are tampered with. There are 4 reports available. A report for the APFlist, the linklist, the LPA list, and a combined report which lists all sensitive data sets. These reports do not give information about how the data sets are protected, nor if they are sufficiently protected.

For RACF systems you can have a look at the RACF RESOURCE category for a report on the protection of these data sets (SENSITIVE PROF), and a list of users with access to them (SENSITIVE TRUST). In addition to these reports the command VERIFY SENSITIVE is available to check the protection, and if necessary generate the RACF commands needed to ensure adequate protection.

Background

The system sensitive data sets are those data sets that need adequate protection to ensure system operation and protection is not disturbed. This includes the APFlist, the linklist, the LPAlist, system parameter libraries, audit trail data sets, system command and system program libraries, page and dump data sets, etc.

The sensitive data set report lists all system-sensitive libraries, and all libraries available on this system but sensitive on another system. The report lists the data sets and the protection required to meet the CS-1 (Commercial Security 1) protection profile from the U.S. Federal Criteria and the draft ISO and Common Criteria. Security zSecure assigns each data set a *sensitivity*, which describes the reason why the data set should be protected, and a *risk*, which describes the lowest access level considered an exposure.

You can add your own data sets by means of the SIMULATE SENSITIVE command (see "SIMULATE" on page 911). You can use SIMULATE SENSITIVE PROCLIB to flag integrity problems for JES2 proclibs used for batchjobs.

Auditing Sensitive Data Sets

The following considerations apply when auditing system-sensitive data sets:

- Ensure the APFlist is up-to-date, for example, all libraries named in the APFlist (and the linklist, if it is authorized) should exist. If a library does not exist, a user could create his own data set, and then rename it to have the name of the missing APF library, thus creating his own authorized programs. In the output of the Sensitive Profiles report such data sets are marked '**notfnd**'.

- Ensure all sensitive data sets are adequately protected and audited. On RACF systems, you can use the Sensitive Trustees and Sensitive Profiles reports to find problems, and the VERIFY SENSITIVE command to fix them.

The batch report to review the sensitive data sets is CKALSENS. The interactive reports are called CKADSEN0 (concise) and CKADSENS (detailed).

The sensitive data sets report can be customized by specifying that all JES2 job proclibs are to be considered sensitive. When using the STATUS AUDIT menu, you can check the option on the customization panel. When generating a report with a batch job, you can include a SIMULATE SENSITIVE PROCLIB command.

After selecting the combined report, the following display appears:

```
All sensitive data sets by priority and type                    Line 1 of 32
Command ===> _____________________________________________ Scroll===> CSR_
                                                  10 Mar 2005 00:07
   Complex  System   Priority Sensitive data sets Audit concerns
   DINO     DINO            5                652              4
   Priority Sensitivity       Sensitive data sets Audit concerns
__        5 NoAPFnoDsn                         2              2
__        2 NoAPFnotMnt                        1              1
__        2 NoAPFnoCtlg                        1              1
__          Active IODF                        1              0
__          APF lib+Lnk                       29              0
__          APF library                       67              0
__          APF Linklst                       29              0
__          APF LPAlist                        2              0
__          Catalog                           53              0
__          HFS dataset                      383              0
__          HSM BCDS                           1              0
__          HSM MCDS                           1              0
__          HSM OCDS                           1              0
__          JES2 Ckpt                          2              0
__          JES2 Spool                         1              0
__          LPA list                          15              0
__          LPA+APF Lnk                        3              0
__          MSTR prmlib                        2              0
__          MSTR STClib                        3              0
__          Pagedataset                        8              0
__          RACF back                          1              0
__          RACF prim                          1              0
__          RMM parmlib                        1              0
__          RMM Control                        1              0
__          RRSFdataset                       24              0
__          Sens Update                        1              0
__          SMF dataset                        3              0
__          SMS ACDS                           1              0
__          SMS COMMDS                         1              0
__          SMS SCDS                           1              0
__          STC joblib                         1              0
__          STC proclib                       11              0
****************************** Bottom of Data ********************************
```

Figure 398. Sensitive data set type overview display

Selecting a record level display (e.g. the Page data sets) yields the following display:

```
All sensitive data sets by priority and type                    Line 1 of 8
 Command ===> _____________________________________________ Scroll===> CSR_
                                                 10 Mar 2005 00:07
    Complex  System   Priority Sensitive data sets Audit concerns
    DINO     DINO            5                652              4
    Priority Sensitivity       Sensitive data sets Audit concerns
             Pagedataset                         8              0
    Pri Dataset                                      VolSer Risk    Audit concer
__      PAGE.DINO.COMMON                                 READ
__      PAGE.DINO.LOCAL1                                 READ
__      PAGE.DINO.LOCAL2                                 READ
__      PAGE.DINO.LOCAL3                                 READ
__      PAGE.DINO.PLPA                                   READ
__      PAGE.MIG014.LOCAL5                               READ
__      PAGE.MIG016.LOCAL7                               READ
__      PAGE.SYS100.LOCAL3                               READ
****************************** Bottom of Data ********************************
```

Figure 399. Sensitive data set display

Table 251 describes the fields of interest in this panel.

Table 251. Sensitive data set display panel - fields of interest

Field	Explanation
Complex	The name of the complex examined.
System	The name of the system examined.
Sensitive data sets	The number of sensitive data sets.
Audit concerns	The number of sensitive data sets for which audit concerns were identified.
Priority	The highest priority for any sensitive data set.
Pri	Numerical audit priority.
Sensitivity	The sensitivity type of the data set. See the fields SENSITIVITY and RISK in “SENSDSN: Sensitive Data Set Names” on page 1255 for a complete list of sensitive datasets and with which access they can be compromised.
Dataset	Data set name.
Volser	Volume serial (blank for VSAM data sets).
Risk	The lowest access level considered a risk.
Audit concern	Audit concerns identified.

Note: The sensitive data set report generates four displays, each slightly different. The preceding display includes the combined display, describing all sensitive data sets. The other displays describe the APFlist, linklist, and the LPAlist. The main difference between the displays is the type of data sets described and the sort order. Also, some fields from the preceding table might be absent and some fields in the following table might be present.

Field	Explanation
APF	Indicates whether the data set is considered APF-authorized on this system. The data set can be on the APF list, on the LPA list, or on the authorized linklist.
APFlist	Indicates whether the data set is on the APF list on this system.
LPA	Concatenation number in the LPA list on this system.
Lnk	Concatenation number in the linklist on this system.

Field	Explanation
Lnkauth	Indicates whether the linklist is authorized (LNKAUTH=LNKLIST) or not.

All fields mentioned in the previous two tables can also be found on the detail display.

AU.C Change track

The interactive component of the Change Tracking system is an ISPF application available under MVS/TSO.

Use Change Tracking to create a verified information base of sensitive RACF profiles, attributes, and other system settings and report on any changes in this information base. The report lists the differences between records in the verified collection and the current system configuration. From the report, you can confirm the changes and update the information in the verified collection with the new information or reject the changes.

The security database records included in the verified collection are data sets that protect APF-authorized libraries and others that your site considers sensitive. To review the list of sensitive resources, see “REPORT_SENSITIVE: Sensitive data sets by profile ” on page 1240. You can monitor other system settings like changes to the list of APF authorized libraries and changes to the RACF Class Descriptor Table. You can track changes to most items that Security zSecure can report information about.

Information is fed to the Change Tracking system by batch housekeeping, which runs Security zSecure to extract system information. You can generate reports from multiple systems, although Change Tracking normally runs on one central system.

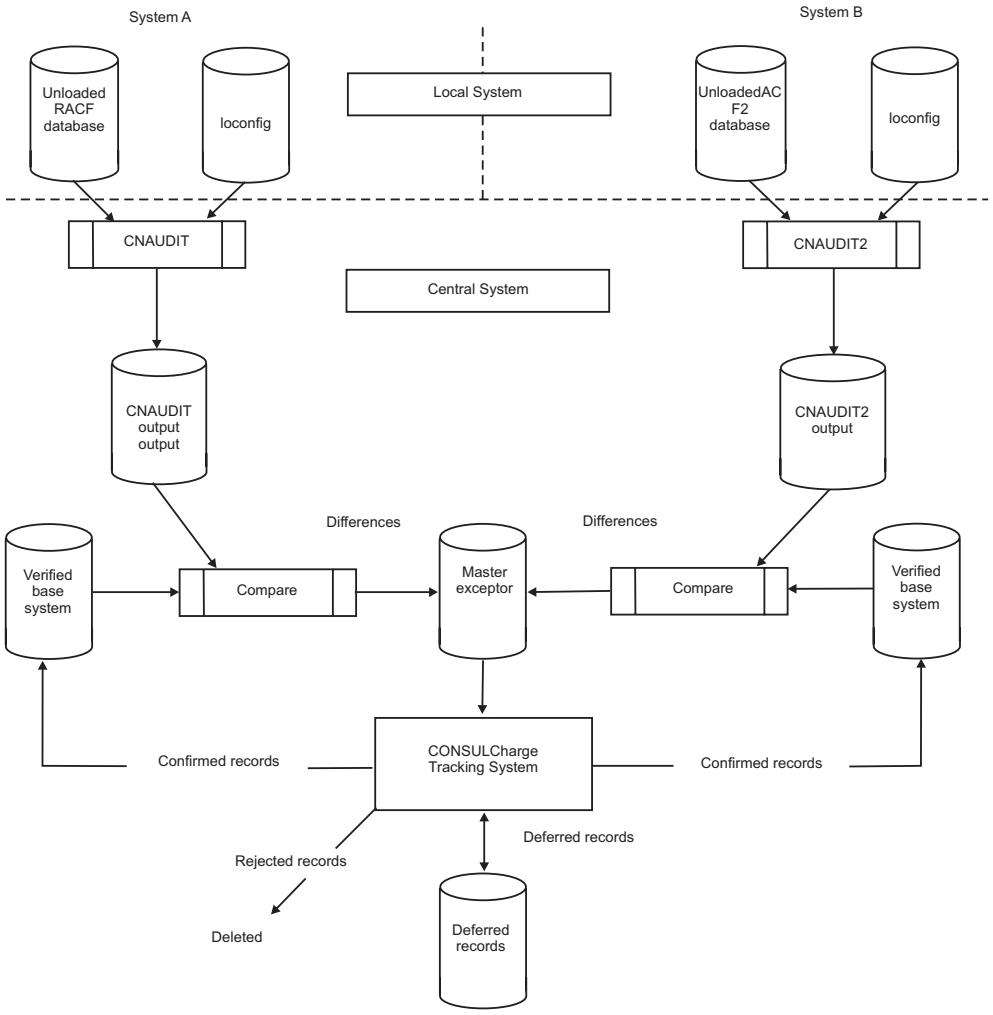


Figure 400. Change Tracking system

The type of information you can monitor depends on the IBM Security zSecure products that are available at your site.

After selecting the **AU.C** Change Track option, a screen is displayed showing all systems that changes are reported for and the date that the batch housekeeping component of Change Tracking ran for each system. The following panel is displayed:

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Change track      Row 1 to 2 of 2
Command ===>                                                Scroll ===> CSR

Enter (E)xceptions or (D)eferred
_ Only select site defined message ids.

  System ID     Date of last run      Days since last run
_  C#M4         14 AUG 2000             1
_  C#M5         14 AUG 2000             2                  *** Warning ***
****************************** Bottom of data ********************************
```

The batch housekeeping component of Change Tracking performs the comparison between the verified base and the current system settings for each system. It is important to run this job daily. If the housekeeping has not run in the previous day for a particular system a `*** Warning ***` message is shown on the right hand side of the display, on the same line as the system name. If you see this message, contact the person who maintains Change Tracking at your site to find out why the housekeeping job did not run.

When you select **Only select site defined message ids**, changes reported because of IBM Security zSecure defined message IDs are not displayed.

The **D** (deferred) action command on the CT system display shows all deferred changes. Processing is similar to **E** (exceptions) processing with the following two differences:

- Only changes in deferred status are displayed
- The D action command is not available. You can not defer a change record that is already in deferred status.

The **E** (exception) action command opens a panel showing all exceptions as shown in Figure 401 shows all exceptions:

```
zSecure Audit Change Tracking - C#M4 Changes              Line 1 of 1610
Command ===> ____________________________________________ Scroll===> CSR_
Enter A(ccept),D(efer),R(eject) or S(how), or primary command "ACCEPT ALL"
   Msg     Description                                                Detai
   C111002 Addition, IPL ALLOCxx suffixes                             00
   C111003 Addition, IPL IEAAPFxx suffix
   C111004 Addition, IPL CLOCKxx suffix                               26
   C111005 Addition, IPL CLPA indicated
   C111006 Addition, IPL Channel Measurement Blocks                   (UNIT
   C111007 Addition, IPL COMMNDxx suffixes                            26
   C111008 Addition, IPL CONSOLxx suffix                              (26,N
   C111009 Addition, IPL COUPLExx suffix                              00
   C111010 Addition, IPL Common Service Area sizes                    (1000
   C111011 Addition, IPL CSCB Location                                ABOVE
   C111012 Addition, IPL Clear VIO
   C111013 Addition, IPL DEVSUPxx suffixes
   C111014 Addition, IPL DIAGxx suffixes                              00
   C111015 Addition, IPL SYS1.DUMPxx data sets                        DASD
   C111016 Addition, IPL DUPLEX paging data set
   C111017 Addition, IPL EXITxx suffixes
   C111018 Addition, IPL IEAFIXxx suffixes                            00
   C111019 Addition, IPL Global Resource Serialization                NONE
   C111020 Addition, IPL GRSCNFxx suffix                              00
   C111021 Addition, IPL GRSRNLxx suffixes
   C111022 Addition, IPL IEAICSxx suffix                              26
   C111023 Addition, IPL IECIOSxx suffix                              26
   C111024 Addition, IPL IEAIPSxx suffix                              26
   C111025 Addition, IPL LNKLSTxx suffixes                            00
   C111026 Addition, IPL Linklist authorized                          YES
```

Figure 401. Change Tracking panel - Detail view

The display has three fields:

Field	Explanation
Msg	The message ID associated with the record.
Description	The description of the message ID.
Details	The details of the change.

A message ID is a 6 digit number preceded with an C or U, describing a record type. Each record type describes a different sort of change to the system. For example, a record that has message id *U000001* can be defined to represent the RACF system special attribute having been added or deleted from a user ID. For instructions on defining messages, see “SE.C SETUP - Change track” on page 1668.

The Description shows details of what the message id means and whether it was an addition or a deletion.

The Details give further information about the record. These vary from message to message.

It is worth bearing in mind that the Change Tracking system reports changes to the configuration system by comparing how the system is currently configured to the verified base. This means that information about the person who made the change is not available. This information is likely to be in the SMF audit trail, which Change Tracking does not read.

Commands on the Change Tracking display

On the Check changes display you can enter the line command (/). The line command displays a pop up window that lists the other line commands shown in the following table.

Command	Meaning	Explanation
A	Accept change	Confirm that the change is correct and authorized and add the record to the verified base.
D	Defer change	Defer the change for future action while you investigate it further or until the situation can be remedied.
S	Show additional information	Show detailed information about the change.
R	Reject change	Reject the change. The record is not added to the verified base. If the situation that caused the record to be reported has not been corrected before the next run of the Change Tracking housekeeping, the change is reported again.

The A, D and R line commands opens a pop-up window, so a change request number or comment text can be entered. Additionally , the R(eject) command opens a pop-up window which suggests the appropriate action to take. A CKGRACF record is written for every Accept, Defer or Reject command that is run.

The primary command ACCEPT ALL accepts all changes. This processing can take a while. For an initial CT run, set the INIT#CT parameter for CT collection job CKAJTSYS to EQ so that all exceptions are written directly to the verified base. The SMF record is only written if IBM Security zSecure Admin is available.

Batch auditing

This manual gives most attention to the Security zSecure ISPF interface. However, the product can also be used in batch mode. The following list describes several ways to use Security zSecure in batch mode. See "Predefined CARLa scripts" for an overview of sample reports.

- The Security zSecure main menu options **AU.L** Libraries, **AU.S** Status, and **EV** Events each have a processing option called either **Run query in foreground or background** or **Run in background**. Selecting a background run enables you to submit a batch job generating the report types selected.
- Main menu option **CO** Commands can be used to submit custom queries or queries from CARLa libraries. The SCKRCARL data set contains many batch reports that can be used or tailored.
- You can create your own JCL submitting a Security zSecure job. The JCL samples in the SCKRCARL data set, or the JCL generated by Security zSecure when you submit a background job can be a good starting point.

  In your own JCL, you can use the INCLUDE command to imbed CARLa scripts from the SCKRCARL data set or your own libraries. You can also use the full Security zSecure language (CARLa) to create your own custom reports.

Predefined CARLa scripts

This section discusses the interactive ISPF and batch reports available in the SCKRCARL library. For information on the naming conventions for CARLa scripts, see "Naming convention" on page 706

Interactive reports

The following interactive (ISPF) system reports are available (these start with CKAD or CKRD):

Report	Meaning
CKAD@MO	Audit concerns from system reports that do not need a CKFREEZE (used to build audit concern overview)
CKAD@XO	Audit concerns from system reports that require a CKFREEZE (used to build audit concern overview)
CKADSCON	System Console Definitions.
CKADSCSM	Globally Modifiable Common Storage Map.
CKADSD80	VM settings audit concerns (80 columns wide). Automatically included by CKRDSD80.
CKADSDMS	DMS system options.
CKADSENS	Sensitive data sets, detailed report.
CKADSEN0	Sensitive data sets, concise report.
CKADSIOA	System Authorized I/O Appendage Table.
CKADSIP	Communications Server IP reports
CKADSIPL	IPL parameters display.
CKADSJC0	JES2 job class parameters, concise report.
CKADSJCL	JES2 job class parameters, detailed report.
CKADSMFS	SMF subsystem settings.
CKADSMNT	Effective UNIX mount points.

Report	Meaning
CKADSMSG	System message-specific data from the Message Processing Facility.
CKADSPC	Program Calls, detailed report.
CKADSPC0	Program Calls, concise report.
CKADSPPT	Program Property Table
CKADSSC0	Subsystem Communication Vector Tables, concise report.
CKADSSCT	Subsystem Communication Vector Tables, detailed report.
CKADSTAP	Tape protection settings (RACF)
CKADSVC	Supervisor Calls, detailed report.
CKADSVC0	Supervisor Calls, concise report.
CKADSVSM	System Virtual Storage Map.
CKADSXIT	Exit and table overview.
CKADSY80	MVS settings audit concerns display (80 columns wide). Automatically included by CKRDSY80.
CKADVOLD	DASD volume protection and sharing.
CKRDSD80	VM settings audit concerns (80 columns wide). Automatically includes CKADSD80.
CKRDSY80	MVS settings and options (80 columns wide). Automatically includes CKADSY80.
CKRDSYSM	System-wide SMF options and settings.

Batch reports

The following batch system reports are available (these start with CKAL, CKAV or CKRL):

Report	Meaning
CKAL$ALL	Collection of all system and many RACF-specific reports.
CKAL$MD	Collection of all system reports that do not require a full CKFREEZE read or RACF database .
CKAL$XD	Collection of all system reports that do require a full CKFREEZE read (but no RACF database).
CKAL@ALL	Overview of audit concerns from all system and many RACF-specific reports.
CKAL@MO	Audit concerns from system reports that do not need a CKFREEZE (used to build audit concern overview)
CKAL@XO	Audit concerns from system reports that require a CKFREEZE (used to build audit concern overview)
CKALSCON	System console definitions.
CKALSCSM	Find globally writable common storage areas (reports on error conditions).
CKALSD13	VM settings audit concerns (132 columns wide). Automatically included by CKRLSD13.
CKALSD80	VM settings audit concerns (80 columns wide). Automatically included by CKRLSD80.
CKALSDMS	DMS system settings.

Report	Meaning
CKALSENS	Four reports on system-sensitive data sets: LPAlist, linklist, APFlist, and all system-sensitive data sets.
CKALSIOA	Authorized I/O appendages.
CKALSIP	Communications Server IP reports
CKALSIPL	IPL parameters listing.
CKALSMNT	Effective UNIX mount points.
CKALSJCL	JES2 job class settings.
CKALSMFS	SMF subsystem options.
CKALSMSG	Message-specific data from the System Message Processing Facility.
CKALSPC	Six reports on Program Calls, showing an overview of audit concerns, a mapping of Linkage Index to Entry Table, a mapping of Entry Table owner to Linkage Index, a system-wide PC routine overview, a non-system-wide PC routine overview, and a detailed view of all PCs sorted by audit priority.
CKALSPPT	Program Property Table.
CKALSSCT	Subsystem Communication Vector Tables.
CKALSTAP	Tape protection settings (RACF)
CKALSVC	Three reports on the SVC table, showing an overview of audit concerns, a summary of the current state of the SVC table, and a detailed view of all SVCs sorted by audit priority.
CKALSVSM	System Virtual Storage Map.
CKALSXIT	Exit and table report.
CKALSY13	MVS settings audit concerns report (132 columns wide). Automatically included by CKRLSY13.
CKALSY80	MVS settings audit concerns report (80 columns wide). Automatically included by CKRLSY80.
CKALVOLD	DASD volume protection and sharing.
CKAVRWWD	Generate UNIX commands to make directories **not** world-writable
CKRLSD13	VM settings audit concerns (132 columns wide). Automatically includes CKALSD13.
CKRLSD80	VM settings audit concerns (80 columns wide). Automatically includes CKALSD80.
CKRLSY13	MVS system settings and options, formatted in 132 columns. Automatically imbeds CKALSY13.
CKRLSY80	MVS system settings and options, formatted in 80 columns. Automatically imbeds CKALSY80.
CKRLSYSM	System-wide SMF options and settings.
C2AL$ALL	Collection of all system and many ACF2-specific reports.

We advise you to run the overall report, CKAL$ALL , at least once. You are then able to decide which reports are useful at your installation, and which sample reports must be edited.

Chapter 6. Library Audit Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

Security zSecure provides library update reports that are used to find and display changes to members of partitioned data sets, as well as changes to a select few sequential data sets and VSAM data sets that you have designated as critical. It handles data sets used on a single system, data sets on shared DASD, and SMS-managed data sets within a sysplex. The reports handle cataloged data sets as well as non-cataloged data sets. The source for these reports are multiple CKFREEZE files for a single system or sysplex; changes can be tracked in the time frame between the dates the earliest and latest CKFREEZE files were generated. (How to create the correct type of CKFREEZE files is discussed later.)

When generating a library update report, Security zSecure starts by tracking the physical data sets over time. It takes into account shared DASD volumes, duplicate volume serials, and duplicate data set names. Tape data sets are supported as well. A simple case of non-SMS-managed volumes is illustrated in Figure 402.

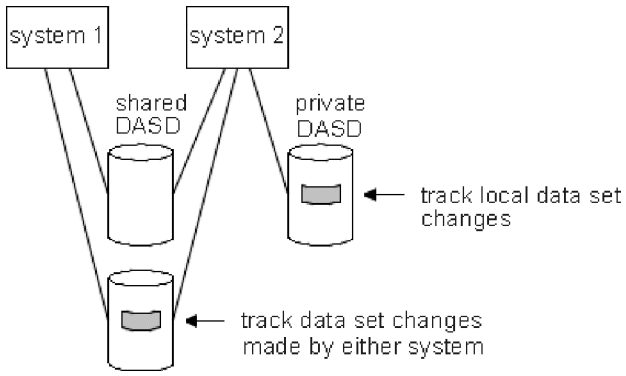


Figure 402. Tracking of data sets

In Figure 402, Security zSecure uses CKFREEZE files from either system to track changes to the data sets on shared DASD and CKFREEZE files from system 2 to track changes to data sets on private DASD.

Security zSecure is also able to track changes to a data set as it is moved from one SMS-managed DASD volume to another. It takes the sysplex name into account; it is safe to mix CKFREEZE files from different sysplexes. Figure 403 on page 530 illustrates tracking SMS-managed data sets.

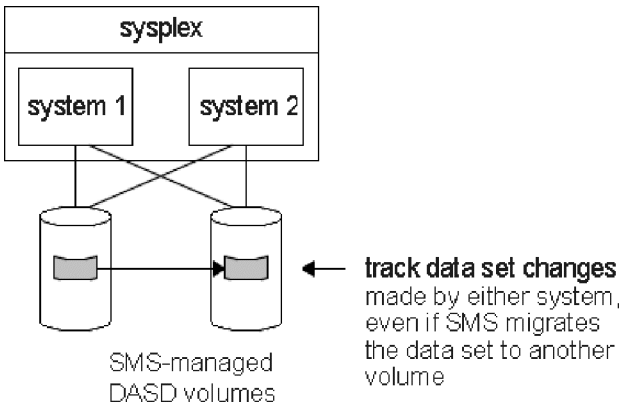


Figure 403. Tracking of SMS-managed data sets

If a data set is moved from a non-SMS-managed DASD volume to an SMS-managed volume, Security zSecure assumes the data set was migrated, and issues warning message CKR0472. This assumption might be false if a data set is deleted and a data set of the same name is later cataloged to an SMS-managed volume.

When the history of the data sets has been determined, Security zSecure tracks changes to data set members. For successive CKFREEZE files that describe the member, the member is compared using a checksum; if no checksum is available, the directory information describing successive members is compared. (A checksum is computed by zSecure Collect, as described later.) In this way, Security zSecure is able to determine during which periods the member was unchanged, and approximately when the member was changed. This is illustrated in Figure 404.

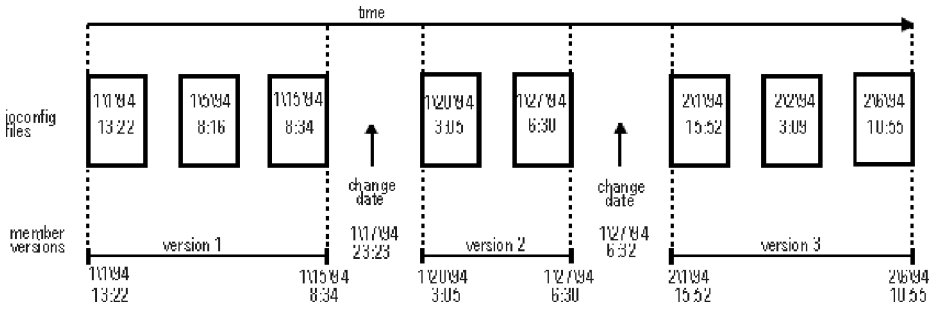


Figure 404. Data set member changes

In Figure 404, Security zSecure splits the history of the member into three periods during which the member was unchanged, each with a start-date and an end-date. Note that the changes to the member were made at some time during the gap between two measurements. In the Security zSecure library update report, a data set member unchanged during a period of time is called a member *version*. Security zSecure reports on these member versions, and the number of changes made over time; for each member version, directory data, checksum data, and instruction/SVC/String scan data can be reported.

All this is more or less true for sequential data sets as well. Checksum data is used from successive CKFREEZE files that describe the data set to determine whether the data set has changed, and approximately when. Of course, since sequential

data sets do not have directories and are not subject to things such as instruction scans, the amount of additional data to be reported on is much more limited than for partitioned data sets.

Preparing CKFREEZE files

The library update report uses CKFREEZE files as its data source. Unlike the other Security zSecure report types, which use one CKFREEZE file per system, the library update report can use several CKFREEZE files per system or sysplex.

When you start using the library update report, your installation procedures might require alteration to maximize the number of generations of CKFREEZE files that are available and online.

You can add CKFREEZE files using the SETUP FILES panel (**SE.1**). New CKFREEZE files can be created using the SETUP NEW panel (**SE.2**), or using the LIBRARY FREEZE panel (option **AU.L.0**).

Figure 405 illustrates how to create a new CKFREEZE file and add it to an existing **Set** of Security zSecure input files. First, go to the LIBRARY FREEZE panel (**AU.L.0**).

```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Audit - Libraries Freeze
Command ===> ____________________________________________________________

Select libraries for digital signature generation:
_  System      - All system sensitive libraries
_  Application - Libraries specified below

Library data set names (fully qualified, no quotes)
Data set name 1 . . . . _____________________________________________
Data set name 2 . . . . _____________________________________________
Data set name 3 . . . . _____________________________________________
Data set name 4 . . . . _____________________________________________
Data set name 5 . . . . _____________________________________________
Data set name 6 . . . . _____________________________________________
Data set name 7 . . . . _____________________________________________
Data set name 8 . . . . _____________________________________________
Data set name 9 . . . . _____________________________________________
Data set name 10  . . . _____________________________________________
```

Figure 405. Library Freeze Menu

In this panel, you can specify the data sets to be frozen. The panel offers the following options:

SYSTEM	Create digital signatures for all system sensitive libraries. This option can be combined with option *APPLICATION*.
APPLICATION	Create digital signatures for the data sets specified on the lower half of the screen. This option can be combined with option *SYSTEM* to create signatures for system sensitive libraries *and* user-specified libraries.

Note that you cannot use this panel to specify sequential data sets for which checksums should be calculated. You cannot do that because this function is typically used in a different way for sequential data sets. For partitioned data sets, changes to members are expected over time, and the main purpose of the library audit function is to monitor these changes. On the other hand, the physical

sequential data sets and VSAM data sets that are important enough to monitor generally do not change much, if at all. The main purpose of calculating a checksum for these data sets is to provide a way to verify that the data set has not been tampered with, typically just before offloading the data to tape.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Audit - Libraries Freeze
Command ===> ____________________________________________________________________

Complete this panel and press ENTER

Optional checksum password   ===> ____________________________________________

Scan string       - List of character values to search in libraries
_____________________________________________________
Scan SVC          - List of supervisor call numbers to search in libraries
_____________________________________________________

Note: type commas between values in the list, e.g. 'SECURITY','BYPASS'
```

Figure 406. Library Freeze Options panel

Optionally, you can supply a checksum password. This can be used to provide virus detection capabilities. See "zSecure Collect command reference" on page 1612. The default for the checksum password is taken from the site-specific string in the CKRSITE module.

Warning: If you change the checksum password, or if you create some CKFREEZE files with checksum passwords and some without, then these files cannot be combined for a library update report.

Additionally, you can specify one or more search strings and calls to one or more Supervisor Service Calls (SVCs) to be searched for in the members for which digital signatures are computed. A Supervisor Service Call (SVC) is a call to a part of operating system that operates in Supervisor state even though called from an unauthorized program.

After you have specified the freeze options, and if either SYSTEM or APPLICATION or both are selected, the data set where the CKFREEZE file is to be stored is created (see Figure 407 on page 533). If the CKFREEZE file already exists, you are prompted to reuse the existing data set or allocate another one.

```
                        zSecure Audit - Setup - New files
Command ===> ____________________________________________________________

CKFREEZE file not found. Change dataset name, or specify allocation parameters

 Dataset name . . . SIGNATUR.CKFREEZE_____________________________________

Allocation parameters to create new dataset:
 Volume serial  . . ______      (Blank for authorized default volume)
 Generic unit . . . ________    (Generic group name)
 Space units  . . . TRKS____    (KB, TRKS, or CYLS)
 Primary quantity . 30______    (In above units, press HELP for suggestion)
 Secondary quantity 30______    (In above units)

 Record format  . . VBS__       (VB or VBS)
 Block size . . . . 27998__
 Logical Record Len X______     (X or maximum record length)



Press ENTER to allocate dataset, press END to stop processing
```

Figure 407. Library Freeze Allocate Data set

On this display, the target data set is specified in which the CKFREEZE file is written. Enter the data set name and press ENTER. If the data set exists, the next panel is displayed; otherwise, you are prompted to correct the data set name or enter allocation parameters. If you press ENTER again without changing the data set name, the data set is allocated. Reasonable allocation parameters are about 2 MB per online DASD volume.

The panel in Figure 408 can be used to review, edit, or submit the JCL. The menu options are not discussed in detail.

```
                        zSecure Audit - Submit menu         Please submit job
Option ===> ____________________________________________________________

1  Browse       Browse JCL
2  Edit         Edit JCL
3  Submit       Submit JCL for execution
4  Cancel       Do not submit the JCL

Job statement information:  (Verify before proceeding)
> //ADGRANTI JOB ,FREEZE,TIME=(10),MSGCLASS=A,NOTIFY=ADGRANT,CLASS=P,_____
> // REGION=32_____________________________________________________________
> /*ROUTE PRINT_____________________________________________________________
> ________________________________________________________________________
```

Figure 408. Library Freeze Submit JCL

After the job has been submitted (e.g. using option **3**), the CKFREEZE file is generated. Wait until the job completes before adding the new CKFREEZE file to a new or existing **Set** of input files. (You can use Security zSecure with an existing **Set** of input files while the CKFREEZE file is generated in the background.) The panel as shown in Figure 409 on page 534 informs you that a job is running, and that the new CKFREEZE file can be used in a new or existing Set of input files, as soon as it has finished. It can be left by pressing ENTER or EXIT.

```
                        zSecure Audit - Setup - New
Command ===> ____________________________________________________________

Datasets will be ready for use after the job completes

Please add any new dataset to a Set of Input Files for use by
zSecure
```

Figure 409. Library Freeze Job Submitted

Interactive Audit Libraries processing

The Audit Libraries application is available using main menu option **AU.L** Audit Libraries. This application allows you to specify selection criteria and then process several CKFREEZE files in the foreground, or submit an equivalent batch job, resulting in a report showing the changed libraries or members. The Audit Libraries panel is displayed in Figure 410.

```
  Menu   Options   Info   Commands   Setup          StartPanel
------------------------------------------------------------------------------
                      zSecure Audit - Audit - Libraries
Command ===> ____________________________________________

0    Freeze          Calculate new digital signatures
1    Lib all         Overview of all libraries
2    Lib changes     Overview of all libraries with changes
3    Status          Show member status
4    Changes         Identify members with changes
5    Scan            Show members flagged by SCAN function
6    Duplicates      Identify identical members
7    Application     Members summarized by application
8    Prefix          Members summarized by member prefix (component code)
9    PTF - ZAP       Members touched by PTF or ZAP
```

Figure 410. Audit Libraries main menu

This first panel offers the following options:

Table 252. Audit Libraries panel - available options

0 FREEZE	Create a new CKFREEZE file. This option has been described in the previous section.
1 LIB ALL	Overview of all libraries and sequential data sets described by the CKFREEZE files. No detail information is included.
2 LIB CHANGES	Overview of the changes in all data sets described by the CKFREEZE files. No detail information is included.
3 STATUS	Show the status of selected members and sequential data sets on or near a particular date.
4 CHANGES	Show all selected changed members and sequential data sets from a specified range of time.
5 SCAN	Show members flagged by the instruction scan or string scan functions.
6 DUPLICATES	Identify identical members. Identical members can be in different libraries and can have different names. Can identify identical sequential data sets too.
7 APPLICATION	Summarize members by application, based on member name prefix.

Table 252. Audit Libraries panel - available options (continued)

8 PREFIX	Summarize members by member prefix, often the product identification.
9 PTF - ZAP	Summarize members by ZAP or PTF id.

For options 2, 4, and 6, CKFREEZE files with digital signatures are required. These files are created with option **0: Freeze**. Alternatively, you can create this type of CKFREEZE file by running zSecure Collect in batch with the CHECK=YES parameter specified. See "zSecure Collect command reference" on page 1612.

For option 9, a CKFREEZE file with IDR information is required. This information is automatically available when CHECK=YES is in effect. Otherwise, you need to specify the zSecure Collect IDR=YES parameter.

For additional information on these options, press PF1 or enter HELP to open the help panel

Selection and options

In this section, the common selection, exclude, and processing options for Audit Libraries reports are discussed. In the next section, the individual reports are discussed.

Select option **3** or **5** to view the common selection panel shown in Figure 411. If you select any of the other options, the resulting panel has fewer fields.

```
                        zSecure Audit - Audit - Libraries Selection
Command ===> ____________________________________________________________________

Select libraries and members that fit all of the following criteria:

Dsname . . . . . _____________________________________________ (EGN mask)
Member name  . . . . . ________
Disk volser  . . . . . ______
Signature status . . . _  Program signed    _  Verification failed
Status at date . . . . __________                    (ddmmmyyyy or yyyy-mm-dd)

Updates between  . . . __________ and __________     (ddmmmyyyy or yyyy-mm-dd)

PTF or ZAP id  . . . . ________

Select Scan results .  /  ScanIns    /  ScanStr    /  ScanSVC
```

Figure 411. Audit Libraries selection menu

This panel, which is common to Audit Libraries menu options **1** to **9**, allows you to specify *selection* criteria. Specify one or more criteria, then press Enter to open the next panel. Libraries and members are selected if they fit *all* of the criteria specified on the Libraries Selection panel.

The **Dsname**, **Member name**, **Disk volser**, and **PTF or ZAP id** fields each accept more than one search string. Each search string can contain generic characters (**%**, * and **) to search for a pattern. To search for an exact string containing these generic characters, enclose the string in single or double quotes. Searching for a substring can be done by prefixing the search string with a colon (**:**).

The **Status at date** and **Updates between** fields accept a date value in either ISO or European date format. The ISO format is `YYYY-MM-DD`, `1999-10-25` for example. The European format is `DDMMYYYY`, `25Oct1999` for example.

Table 253 provides the field descriptions for the Library selection panel.

Table 253. Library selection panel - field descriptions

Field	Description
Dsname	Fully qualified data set name, or a pattern.
Member	Member name. Library reports only include libraries for which at least one member matches the name specified; member reports only include members matching the name specified.
Disk volser	Volume serial number. You should take care with this option when reporting on SMS-managed data sets, as these data sets can change their volume serial over time.
Signature status	Indicates whether a module has the signed attribute set and whether signature verification for the module failed. If the module is signed, select **Program signed**. If the module failed signature verification, select **Verification failed**.
Status at date	For each member, select the version at this particular date. If the date falls in between two freeze dates, and the member has changed in the interim period, the version immediately following the date specified is selected.
Updates between	Select only those data sets that have changed during the period of time specified.
PTF or ZAP id	Select members that contain the particular PTF or ZAP id specified. (For a library report: select only libraries with one or more members containing the PTF or ZAP id.)
ScanIns	Select members in which any of the following instructions were found: BypassSAF, FakeAPF, FakeOper, FakePriv, FakeSpec, KeyzeroRB or ModeSupRB. It is only available if the CKFREEZE file used was produced with parameters `SCAN=YES` and `CHECK=Y` or `CHECKDSN=Y` specified. This field is only present when Status or Scan has been selected.
ScanStr	Select members in which a user specified string was found. It is only available if the CKFREEZE used was produced with parameters `SCAN=YES`, `CHECK=Y` or `CHECKDSN=Y` and `SCANSTR` arguments specified. This field is only present when Status or Scan has been selected.
ScanSVC	Select members in which a user specified SVC call was found. It is only available if the CKFREEZE used was produced with parameters `SCAN=YES`, `CHECK=Y` or `CHECKDSN=Y` and a `SCANSVC` list specified. This field is only present when either the Status or Scan field has been selected.

After pressing Enter on the selection panel, the *exclude* panel in Figure 412 on page 537 is displayed.

```
                    zSecure Audit - Audit - Libraries Exclusion
Command ===> ____________________________________________________________

Exclude libraries and members that fit all of the following criteria:

Dsname . . . . . . . . ____________________________________________ (EGN mask)
Member name  . . . . . ________
Disk volser  . . . . . ______

Updates between  . . . __________ and __________     (ddmmmyyyy or yyyy-mm-dd)
```

Figure 412. Audit Libraries exclusion menu

This panel allows you to specify *exclusion* criteria. Libraries and members selected by the criteria from the previous panel are excluded if libraries or members fit *any* of the criteria specified on this panel. The exclusion criteria are specified in the same way as the selection criteria on the previous panel.

The panel in Figure 413 is the report parameters panel. It is common to all Audit Libraries menus and is the last panel before processing is started.

```
                    zSecure Audit - Audit - Libraries Options
Command ===> ____________________________________________________________

Select options for Library update report:

Show output in DISPLAY or LIST format  . .  DISPLAY__    (Display/List)

Run query in Foreground or Background  . .  FORE_____    (Fore/Back)

Level of detail in reports . . . . . .  DETAILED_    (Concise/Detailed)
```

Figure 413. Audit Libraries report parameters panel

This panel allows you to specify the following processing parameters:

Show output in DISPLAY or LIST format
This option determines whether the data selected is shown in an interactive display (DISPLAY, when running interactive) or in a printable report format (LIST). When memory is tight, or if the output is to be printed, the concise format is preferable. When a small amount of data is selected that must be studied in detail, select the DISPLAY and DETAILED options.

Run query in Foreground or Background
This option determines whether Audit Libraries processing is to proceed in the foreground, or whether to submit a background (batch) job.

Level of detail in reports
This option determines the level of detail in the reports generated. The only report affected at this time is the DUPLICATES report.

If foreground processing is selected, Security zSecure starts processing after Enter is pressed on the processing options panel. During processing, the number of CKFREEZE records read is displayed. After processing, the resulting output is displayed. Processing can be halted by pressing the ATTN key.

If background processing is selected, the usual SUBMIT panel is displayed, allowing you to browse or edit the JCL generated, and then submit a batch job.

Audit Libraries reports

This section describes the reports available using Audit Libraries menu options **1** to **9**. No selection, exclude, or processing option displays are shown; see the previous section for an explanation of those displays.

Option **1** LIB ALL shows an overview of all libraries and sequential data sets described in the CKFREEZE files used, which match the selection and exclude criteria specified. The report shows the data sets selected for each data set with an indication of its type, the number of members found (1' is shown for sequential data sets), the number of changed members or changes to sequential data sets, and the number of members added and deleted. The changed, added, or deleted members are listed as detail information, but no further information for the members is included. A sample batch report is included in Figure 414.

```
Overview of library status

Dataset                                   DS  Memb Member    Chgs  Adds  Dels
SYS1.CICS9103.CICSLPA                     PO     2              2     0     0
                                                   DFHIRP       1     0     0
                                                   DFHPXR       1     0     0
SYS1.VSF2COMP                             PO     4              2     0     0
                                                   FORTVS2      1     0     0
                                                   ILX0TRCE     1     0     0
```

Figure 414. Batch LIB ALL Report

Note that data set SYS1.VSF2COMP has 4 members, but only 2 were changed; the unchanged members are not listed.

Option **2** LIB CHANGES is equivalent to option **1**, but only shows data sets with changes. The reports generated by options **1** and **2** have the same layout.

Option **3** STATUS shows the status of selected members and sequential data sets. It includes detail information for each member, and requires more memory than the previous reports; you are advised to specify strict selection criteria. The resulting reports are split into load-libraries, non-load-libraries, and sequential data sets; each report includes data set names, and, where applicable, the selected member names and detail information for each member. If a member was changed, multiple versions can be included in the report. The DISPLAY version of the report is shown in Figure 415, starting with the data set overview display.

```
Load libraries with member level information                    Line 1 of 4
Command ===> ____________________________________________________ Scroll===> CSR
                                          8 Mar 2001 13:56
   Dataset                                Members ScanSVC ScanStr ScanIns
s_ BFS.SBFSLMOD                                 4       2       3       1
__ SYS1.SVCLIB                                  4       0       0       0
__ SYS1.VTAMLIB                               350      12       6      13
__ SYS1.V2R8M0.SHASLINK                        33       3       3       2
****************************** BOTTOM OF DATA ********************************
```

Figure 415. Library Status data set display

This display shows the data sets with members matching the search criteria, and the number of members found.

Select any data set for an overview of members.

```
Load libraries with member level information                    Line 1 of 4
Command ===> ____________________________________________ Scroll===> CSR
                                        8 Mar 2001 13:56
   Dataset                              Members ScanSVC ScanStr ScanIns
   BFS.SBFSLMOD                               4       2       3       1
   Member   Num Size (Kb) LKED date APF AC1 RENT  PSg PSp InstrSc Str SVC found:
s_ BFSMCMD    1       314 07Oct1999 Yes No  Yes                   Yes Yes
__ BFSMFMT    1       165 07Oct1999 Yes No  Yes                   Yes  No
__ BFSMFRVD   1         5 07Oct1999 Yes No  Yes                    No  No
__ BFSMSRV    1      4023 07Oct1999 Yes Yes Yes                0   Yes Yes
****************************** BOTTOM OF DATA ********************************
```

Figure 416. Library Status member display

The member display shows the members that fulfill the filter criteria, and includes the size in kilobytes, linkage-edit date, and the results of an instruction and string scan.

Select any member for a detailed member display.

```
Load libraries with member level information                    Line 1 of 9
Command ===> ____________________________________________ Scroll===> CSR
                                        8 Mar 2001 13:56
 Dataset                              Members ScanSVC ScanStr ScanIns Authorized
  ASM.SASMMOD1                             18       0       0       1 Yes
  Member   Num Size (Kb) LKED date APF AC1 RENT PSg PsP InstrSc Str SVC found:
  ASMADOP    1        64 30Apr2008 Yes No  Yes                   No  No


 Member version lifetime
 Start date                  29Jul2008
 End date                    29Jul2008
 Changed between                       and 29Jul2008

 Member properties
 Application                 High level assembler/ High level assembler toolkit
 Identify data
 ZAP data
 Program signed              No

 Audit findings
 Signature verification failed No
 Instruction Scan Results
 String Scan Results         No
 SVC Scan Results
****************************** BOTTOM OF DATA ********************************
```

Figure 417. Library Status detail member display

Option **4 CHANGES** is equivalent to option **3 STATUS**, but includes only the *changed* members matching the selection criteria specified. The Status and Changes reports have a similar layout, but the Changes report includes the earliest and latest linkage-edit dates found.

Option **5 SCAN** reports on members with instruction scan or string scan results. The resulting report has the same layout as the Status report.

Option **6 DUPLICATES** reports on duplicate load modules, which can reside in different data sets and can have different names. Additionally, you can use this option to check whether two sequential data sets are identical, assuming that the checksum data for both data sets is present in the `CKFREEZE` file. When you run the Duplicates report, use only one `CKFREEZE` file for the input data source. A sample batch report is included in Figure 418 on page 540.

```
Identical members, load modules

  DSNs Member   First lked Last lked Dataset                        VolSer LKED date AC1 APF RENT NX  OL  REUS Rmode
               22Jan1993  18Feb1994
     2 IEFBR14  18Feb1994  18Feb1994
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
                                    SYS1.LPALIB                    S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
     1 BREAKPT  22Jan1993  22Jan1993
                                    C#MA.CRMPROD.LOAD              SYST10 22Jan1993 No  Yes Yes  No  No  Yes  24
     1 ERBMFDUC 18Feb1994  18Feb1994
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
     1 ERBMFIUC 18Feb1994  18Feb1994
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
     1 ERBMFRUR 18Feb1994  18Feb1994
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
     1 ERBMFTUR 18Feb1994  18Feb1994
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  No  Yes  24
               14Jun1990  12Apr1994
     4 IEV80    14Jun1990  12Apr1994
                                    C#MA.CRMPROD.LOAD              SYST10 14Jun1990 No  Yes Yes  No  No  Yes  24
                                    IPO1.LINKLIB                   M93113 12Apr1994 No  Yes Yes  No  Yes Yes  24
                                    IPO1.LINKLIB                   S9311A 12Apr1994 No  Yes Yes  No  Yes Yes  24
                                    SYS1.LINKLIB                   S9311A 18Feb1994 No  Yes Yes  No  Yes Yes  24
```

Figure 418. Batch DUPLICATES Report

The report displays members with identical content (but maybe different names) sorted on member name; for each duplicate, the member names, data set names, PTF, and ZAP ids are included. This option allows you to find duplicates of e.g. AMASPZAP and IEFBR14.

Option **7** APPLICATION is used to summarize the members selected by (guessed) application, based on the member name prefix. A sample batch report is included in Figure 419 on page 541.

```
Applications in libraries based on membername prefix

                              Member   LKED date PSg PsP
Assembler-H
        C#MA.CRMPROD.LOAD
                              IEV00    14Jun1990
                              IEV10    14Jun1990
                              IEV20    14Jun1990
                              IEV50    14Jun1990
                              IEV60    14Jun1990
                              IEV80    14Jun1990
                              IEV90    14Jun1990
        IPO1.LINKLIB
                              IEV00    14Jun1990
                              IEV10    14Jun1990
                              IEV20    14Jun1990
                              IEV50    14Jun1990
                              IEV60    14Jun1990
                              IEV80    14Jun1990
                              IEV90    14Jun1990
        SYS1.LINKLIB
                              IEV00    12Apr1994
                              IEV10    12Apr1994
                              IEV20    12Apr1994
                              IEV50    12Apr1994
                              IEV60    12Apr1994
                              IEV80    12Apr1994
                              IEV90    12Apr1994
ACF/VTAM Virtual Telecomm Access Method
        M9311.T#D.VTAMLIB
                              ISTINCLM 18Mar1994
                              ISTMGC00 01Mar1994
                              ISTSDCOS 01Mar1994
        SYSP.VTAM.P.VTAMLIB
                              ISTEXCCS 18Oct1994
                              ISTINCLM 26Mar1997
                              ISTSDCOS 26Mar1997
        SYS1.LINKLIB
                              ISTCPCRY 18Feb1994
                              ISTCPCSF 18Feb1994
                              ISTDINFO 18Feb1994
                              ISTIECVR 18Feb1994
```

Figure 419. Batch APPLICATION Report

The report is sorted by application name; for each application, the data sets, and members are included. If Security zSecure is not able to derive the application name, the member is suppressed. See the PREFIX report (option **8**) for an alternative.

Option **8** PREFIX is used to summarize the members by their prefix, which often indicates the product id. A sample batch report is included in Figure 420 on page 542.

```
Mem                              Member   LKED date PSg PsP
IEW Linkage Editor and Loader
            C#MA.CRMPROD.LOAD
                                 IEWL
                                 IEWLDRGO
                                 IEWLF128
                                 IEWLF440
                                 IEWLF880
                                 IEWLOAD
                                 IEWLOADR
            IPO1.LINKLIB
                                 IEWL
                                 IEWLF128
                                 IEWLF440
                                 IEWLF880
            SYS1.LINKLIB
                                 IEWBLDGO
                                 IEWBLINK
                                 IEWBLOAD
                                 IEWBLODI
IFA SMF Dump Program (IFASMFDP)
            SYS1.LINKLIB
                                 IFAEASIL
                                 IFAPCWTR
                                 IFASMF
                                 IFASMFDP
                                 IFASMFDT
```

Figure 420. Batch PREFIX Report

The report is sorted by prefix name; for each prefix, the application, data sets, and members are included. The main difference with option **7** APPLICATION is that those products for which Security zSecure does not derive an application are included.

Option **9** PTF - ZAP is used to summarize the members selected by PTF or ZAP id application. The resulting report is split into a report summarizing PTF ids and a report summarizing ZAP ids. The report does not contain detailed information for the members. A sample batch report summarizing PTF ids is included in Figure 421.

```
Occurrence of ZAPs in libraries

         Dataset                                      Member   LKED date
PICF212
         C#MA.CRMPROD.LOAD
                                                      CNF212   27Oct1993
         C#MA.CRMTEST.LOAD
                                                      CNF211   20Sep1993
                                                      CNF212   14Jun1994
PR31041
         SYSAPPL.CNRACF.SC2RLOAD
                                                      CNARACF  14Jun1994
                                                      CNAUDIT  14Jun1994
                                                      CNRACF   14Jun1994
PR31116
         SYSAPPL.CNRACF.SC2RLOAD
                                                      CNARACF  14Jun1994
                                                      CNAUDIT  14Jun1994
                                                      CNRACF   14Jun1994
```

Figure 421. Batch PTF - ZAP Report

The report is sorted by PTF id; for each id found, the report includes the data set names, the members in each data set that contain the ZAP or PTF, and the linkage-edit date of the load module.

Predefined CARLa scripts

In this section, the sample reports available in the SCKRCARL library are discussed. The convention used to name CARLa scripts is explained in "Naming convention" on page 706

Batch reports

The following batch library audit reports are available. (These start with CKALM.)

Report	Meaning
CKALMAPP	Applications in libraries based on membername prefix (cf. **AU.L.7**)
CKALMCHG	Details of libraries with member level changes (cf. **AU.L.4**)
CKALMDET	Details of libraries with member level information (cf. **AU.L.3**)
CKALMDUP	Identical members in libraries (cf. **AU.L.6**)
CKALMID	Identify ZAPs and identify data in libraries (cf. **AU.L.9**)
CKALMOV	Overview of library status (cf. **AU.L.1**)
CKALMOVC	Overview of library changes (cf. **AU.L.2**)
CKALMPRF	Applications in libraries by component code (cf. **AU.L.8**)

AU.L.5 is not represented separately. Essentially it is the same as **AU.L.3** with a different selection. These reports are a functionally stabilized set of sample CARLa scripts. These samples are not directly used in the interface; use the COMMANDS file on the RESULTS panel after a query to verify the exact CARLa used.

These samples refer to the NEWLIST NAME=LIBSEL statement with a LIKELIST=LIBSEL clause. Make sure that either a NEWLIST with that name and the appropriate selections is included in the query ahead of them, or specify SUPPRESS MSG=403. See also "Selecting based on previously specified criteria (LIKELIST)" on page 887 and "Using record display scripts for interactive reporting" on page 591.

Chapter 7. SMF and HTTP Reporting (Events menu)

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

zSecure provides record processing and reporting for the following types of SMF and HTTP data:

- live SMF data sets
- SMF log streams
- sequential SMF data that has been produced by the `IBM IFASMFDP` or `IFASMFDL` programs
- HTTP access, error, or site-defined log files

This data can be useful for monitoring user activity and MVS events.

For details on SMF processing, select one of the following topics:

- "Selecting and dumping SMF data sets"
- "Using Security zSecure to process SMF data instead of IFASMFDFP" on page 549
- "Interactive SMF processing for RACF" on page 550
- "Batch SMF processing" on page 589
- "SMF reporting using predefined CARLa scripts" on page 590

Selecting and dumping SMF data sets

You select the SMF data source for reporting from the SETUP options available from the Main menu. (**SE.1**). The data source is defined by an input set which can include one or more files containing the data for reporting. You can either create an input set for the SMF data sources or add them to an existing input set. You can use any of the following types of data sets or files for the SMF input:

- Live SMF data
- Fully qualified data set names, or relative GDG generations
- SMF log streams
- A GDG base name to allocate all generations of a GDG

When you specify the data set or file information, you must ndicate the data type. Table 254 lists the supported data types for SMF input sources.

Table 254. Data set types for SMF input data sources

SMF data	Input set TYPE value	Example
VSAM data sets or dumped non-VSAM data sets	SMF	See "Specifying a dumped SMF data set or a live SMF data set from another system" on page 547.
Live SMF	ACT.SMF	See "Specifying a live SMF file" on page 546.
SMF log streams	SMF.LOGSTR	See "Specifying SMF log stream input data" on page 548.

Table 254. Data set types for SMF input data sources (continued)

SMF data	Input set TYPE value	Example
SMF data sets on tape	SMF	See "Specifying SMF data sets on tape" on page 548.

You can use Security zSecure to unload live data sets and also any local unloaded SMF data available online. See "Using Security zSecure to process SMF data instead of IFASMFDFP" on page 549. For information about which record types to use, see "Adding SMF data sources to input file sets." If you have any local unloaded SMF data available online, you can also read this data set using Security zSecure.

Adding SMF data sources to input file sets

Use the Setup Input Files menu option to add the SMF input data sets or files and select them for processing.

To use this function, select the Setup Input Files menu option available from the Main menu (SE.1) or type SETUP FILES on the command line. When you select this option, the Setup - Input files panel shown in Figure 422 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Setup - Input files
Command ===>                                                 Scroll ===> CSR

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

  Description                                                Complex
_ Active primary RACF data base                              C##4     selected
_ Active backup RACF data base                               C##4
_ Active backup RACF data base and live SMF data sets        C##4
_ smf copy on disk + ckfreeze + unload                       testcomp
****************************** BOTTOM OF DATA ********************************
```

Figure 422. Setup Input files

The Setup - Input files panel shows a list of the input sets that are currently defined.

From this panel, you can do the following:

- Use the **I** line command to add a new input set.
- Use the **E** line command to edit an existing input set.

For more information, see "SE.1 Setup - Input files" on page 1645 and the *IBM Security zSecure Admin and Audit for RACF: Getting Started Guide* Guide.

Specifying a live SMF file

To specify a live SMF file, do the following:

1. Follow the procedure to add a data source "Adding SMF data sources to input file sets."
2. When you get to the step to specify the information for the live SMF file, type `ACT.SMF` in the **Type** column as shown in Figure 423 on page 547.

Specifying a data set name for a live SMF data source is optional. READ access to the SMF recording data sets is required.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                  zSecure Suite - Setup - Input files
Command ===> ____________________________________________ Scroll ===> CSR

Description . . . . smf copy on disk + ckfreeze + unload_____________________
Complex . . . . . . C##4
RRSF node . . . . . ________   Local node for RRSF

Enter data set names and types.       Type END or press F3 when complete.
End dsname with .* to get a list.     Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D          Type REFRESH to submit unload job.

  Data set name or DSNPREF= or Unix file name             Type        NJE node
_ 'S##APPL.CNAUDIT.UNLOAD'_____________________________ UNLOAD_____ ________
_ 'S##APPL.CNAUDIT.CKFREEZE'___________________________ CKFREEZE___ ________
_ _____________________________________________________ ACT.SMF     ________
****************************** Bottom of data ********************************
```

Figure 423. Specifying a live SMF file

Specifying a dumped SMF data set or a live SMF data set from another system

To specify a dumped SMF data set or a live SMF data set from another system, do the following:

1. Follow the procedure to add a data source "Adding SMF data sources to input file sets" on page 546.
2. When you get to the step to specify the information for the live SMF file, type SMF in the **Type** column.
3. Type the enter the fully qualified data set name as shown in Figure 424.

You can also use the DSNPREF= option to specify a collection of SMF input data sets that begin with a specified high-level qualifier. For example, specifying DSNPREF=SYS1.DAILY.SMF specifies all data sets that begin with *SYS1.DAILY.SMF*. The last qualifier specified is interpreted as a partial qualifier. To match only full qualifiers end the DSNPREF value with a period.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                  zSecure Suite - Setup - Input files
Command ===> ____________________________________________ Scroll ===> CSR

Description . . . . smf copy on disk + ckfreeze + unload_____________________
Complex . . . . . . C##4
RRSF node . . . . . ________   Local node for RRSF

Enter data set names and types.       Type END or press F3 when complete.
End dsname with .* to get a list.     Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D          Type REFRESH to submit unload job.

  Data set name or DSNPREF= or Unix file name           Type        NJE node
_ 'SYSAPPL.CNAUDIT.UNLOAD'_____________________________ UNLOAD_____ ________
_ 'SYSAPPL.CNAUDIT.CKFREEZE'___________________________ CKFREEZE___ ________
_ 'R#OPROB.R#93278.SMF'________________________________ SMF________ ________
****************************** Bottom of data ********************************
```

Figure 424. Specifying a dumped SMF file

Specifying SMF log stream input data

To specify a dumped SMF data set or a live SMF data set from another system, do the following:

1. Follow the procedure to add a data source "Adding SMF data sources to input file sets" on page 546.
2. When you get to the step to specify the information for the file, type `SMF.LOGSTR` in the **Type** column.
3. Then, type the data set name as `logstream_name('time','SID(sysid)')`, where `time` and `sysid` are optional.

   The following examples show valid specifications for the data set name.

   - `IFASMF.TYPE80` or
   - `IFASMF.TYPE80('DURATION=(24,HOURS)')` or
   - `IFASMF.TYPE80('FROM=(2007/288),TO=(2007/288),LOCAL','SID(IPO1)')`

Specifying SMF data sets on tape

You can also specify multiple SMF data sets and GDG names for SMF reporting.

1. Follow the procedure to add a data source "Adding SMF data sources to input file sets" on page 546.
2. Type `SMF` in the **Type** column.Figure 425 illustrates how you specify multiple SMF data sets and GDG names.

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                  zSecure Suite - Setup - Input files
Command ===> ____________________________________________ Scroll ===> CSR

Description . . . . smf copy on disk + ckfreeze + unload_____________________
Complex . . . . . . C##4
RRSF node . . . . . ________   Local node for RRSF

Enter data set names and types.       Type END or press F3 when complete.
End dsname with .* to get a list.     Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D          Type REFRESH to submit unload job.

  Data set name or Unix file name                        Type        NJE node
_ 'SYSAPPL.CNAUDIT.UNLOAD'_____________________________ UNLOAD____ ________
_ 'SYSAPPL.CNAUDIT.CKFREEZE'___________________________ CKFREEZE___ ________
_ 'R#BB.SMFMVS(0)'_____________________________________ SMF_______ ________
_ 'R#BB.SMFMVS(-1)'____________________________________ SMF_______ ________
_ 'R#BB.SMFMVS(-2)'____________________________________ SMF_______ ________
****************************** Bottom of data ********************************
```

Figure 425. Specifying SMF files using GDG names

3. After you enter the data set or tape names, type SAVE on the command line to save the input set.

To use this input set for reporting, submit a batch job using the **CO** option available on the main menu. For details, see "Batch SMF processing" on page 589. If you have MOUNT authority, you can use this input set for interactive reporting but we do not recommend it.

Selecting HTTP and user-defined logs

You can create reports for HTTP and user-defined logs by selecting an HTTP or user-defined log file as an input source. You can generate reports on the following log types:

- WEBACCESS for HTTP access logs

- WEBERROR for HTTP error logs
- Site-defined log types (See “SE.U SETUP - user-defined input sources” on page 1667.)

SMF log files can also be read directly from a UNIX file system.

1. Add a data source. (See “Adding SMF data sources to input file sets” on page 546).
2. In the **Type** field, type one of the input file types for HTTP logs. To read files directly from UNIX, specify the full path name under **Data set** or **Unix** file name.

Figure 426 shows an example that adds two HTTP log data sources to an input set.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                    zSecure Suite - Setup - Input files        Row 1 from 6
Command ===> _____________________________________________ Scroll ===> CSR

Description . . . . DAILY BACKUP with SMF and HTTP logs_____________________
Complex . . . . . . C##4____
RRSF node . . . . . ________   Local node for RRSF

Enter data set names and types.         Type END or press F3 when complete.
Enter dsname with .* to get a list      Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D            Type REFRESH to submit unload  job.

   Data set or Unix file name                                Type        NJE node
_  'C##A.X.HTTP53.LOG'_____________________________________ WEBACCESS   ________
_  /u/c##a/httplogs/errorlog_______________________________ WEBERROR    ________
_  'S##APPL.CNAUDIT.UNLOAD'________________________________ UNLOAD      ________
_  'S##APPL.CNAUDIT.CKFREEZE'______________________________ CKFREEZE    ________
_  'C##A.X.D##4.D2001W18.SMF'______________________________ SMF         ________
****************************** Bottom of data ********************************
```

Figure 426. Specifying HTTP logs

Using Security zSecure to process SMF data instead of IFASMFDFP

You can use the RACF SMF data unload utility IFASMFDP to read any VSAM or non-VSAM SMF data set and write selected records to a sequential file. You can process the sequential file using Security zSecure. However, you can also read SMF data (both live and unloaded) directly with zSecure instead of using IFASMFDP. For example, the zSecure job C2RJFUNL reads live SMF, selects and then rewrites specific record types. The resulting data set can be blocked efficiently and contains fewer records than the IFASMFDP output file. You can improve processing speed by using the zSecure data set as the data source.

You can also customize the selection of SMF records in the C2RJFUNL job. For example, the SMF record types that DFSMShsm writes are customizable. If you want to include DFSMShsm daily statistics or functional statistics records in your selection, add the SMF record type for DFSMShsm in job C2RJFUNL. The record type number for the statistics records is one more than the value specified in the SETSYS SMF command in DFSMShsm's configuration.

Interactive SMF processing for RACF

The SMF processing application is available from the Events options (**EV**) on the main menu. Use these options to specify the audit selection criteria for creating reports on the SMF record types, user or group event records for example. Depending on the options you specify, the data can be processed in the foreground on the ISPF panels or you can submit an equivalent batch job. The report results are sent to the ISPF display or a printed report depending on the options specified in the selection panels.

Figure 427 shows the main menu for Events.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Events
Option  ===>_____________________________________________________________________

SE   Setup           Options and input data sets
RA   RACF            RACF Administration
AU   Audit           Audit security and system resources
EV   Events          Event reporting from SMF and other logs
  U    User            User events from SMF
  G    Group           Group events from SMF
  D    Data set        Data set events from SMF
  R    Resource        General resource events from SMF
  F    Filesystem      Unix filesystem events from SMF and other logs
  I    IP              IP events from SMF and other logs
  1    SMF reports     Predefined analysis reports
  2    RACF events     RACF logging for specific events
  4    DB2             DB2 events from SMF
  5    CICS            CICS monitor records from SMF
  6    Omegamon        Omegamon events from SMF
  C    Custom          Custom report
CO   Commands        Run commands from library
IN   Information     Information and documentation
LO   Local           Locally defined options
X    Exit            Exit this panel

Input complex: Active backup RACF data base and live SMF data sets

Product/release:
5655-T01 IBM Security zSecure Admin
5655-T02 zSecure Audit for RACF 1.13.0
```

Figure 427. EVENTS main menu

Table 255 lists the Events menu options and descriptions.

Table 255. Events menu options and descriptions

Event Function	Description
U User	Select and list SMF records concerning specific users. See “Reporting on user events (EV.U)” on page 564.
G GROUP	Select and list SMF records concerning specific groups. See “Reporting on group events (EV.G)” on page 565.
D Data set	Select and list SMF records concerning specific data sets. See “Reporting on data set events (EV.D)” on page 566.
R Resource	Select and list SMF records concerning specific resources. See “Reporting on general resource events (EV.R)” on page 567.
F Filesystem	Select and list log records (SMF and other) concerning USS files. See “Reporting on Unix file system events from SMF and other logs (EV.F)” on page 568.

Table 255. Events menu options and descriptions (continued)

Event Function	Description
I IP	Select and list log records (SMF and other) concerning IP addresses and connectivity statistics. See “Reporting on IP events from SMF and other logs (EV.I)” on page 569.
1 SMF reports	Run predefined analysis reports. See “Logging for specific RACF events (EV.2 - RACF EVENTS)” on page 578.
2 RACF events	Select and list RACF processing records to trace specific event types, such as access violations or use of RACF commands. See “Logging for specific RACF events (EV.2 - RACF EVENTS)” on page 578.
4 DB2	Select and list SMF records concerning DB2. See “Reporting on DB2 EVENTS (EV.4)” on page 570.
5 CICS	Select and list SMF records concerning CICS monitoring information. See “Reporting on CICS monitoring events (EV.5)” on page 571.
6 Omegamon	Select and list SMF records for Omegamon events. See “Reporting on Omegamon events (EV.6)” on page 572.
C Custom	Specify custom queries that do not fit the standard criteria of the other options. Use this option to create custom report displays and to create summaries. You can also use the predefined report layouts that are used by the other menu options. See “Creating custom queries and reports (EV.C CUSTOM)” on page 586.

For additional information about the Event menu options, use the F1 function for help on a field or panel.

Querying SMF data

The following procedure provides instructions for querying SMF data for information about user, group, data set, general resource, Unix filesystem, IP, DB2 and CICS monitoring.

1. Select the Events menu option for the information type you are interested in. For example, if you want to investigate user events, type **EV.U** on the command line.
2. On the selection panel, enter the base selection criteria for the query as described in Table 256.

Table 256. Specifying selection criteria for SMF records

To select ...	Do this ...
Select all SMF records that have information related to the specified event (user, group, DB2, CICS monitoring, for example)	Leave the fields on the record selection panel blank, then press **Enter** to show the records.
Select SMF records based on user-specified search criteria	Select one or more fields on the record selection panel. Then, press **Enter** to show the list of records matching the selection criteria.
Select SMF records using search filters.	In some selection fields, you can enter a filter. For example, on the User Events - Record panel, you can select all records that relate to actions performed by users that have the characters C##QAO in the first 6 positions by typing `C##QAO*` in the user ID field.

3. Optionally, you can specify advanced selection criteria to further qualify the SMF record selection.
   - Type / in the input field for each advanced selection criteria option you want to use.
   - At the prompt, specify the criteria for each of the advanced options you selected on the report selection panel. For details, see "Specifying advanced selection criteria for SMF records."
4. Specify the Output/Run options.

   Use the **Output/run** options for configuring any of the Event selection panels. The selections you specify are saved to your ISPF profile and become the default setting for all the selection panels. As a result, you can set an option one time (**Output in print format**, for example) and use it for all SMF event reporting. For details on these options, see "Selecting Output/run options" on page 562.
5. After you specify the selection criteria and output and run options, press **Enter** to process the query.

   If you have selected any of the advanced selection criteria options, a series of panels opens so you can specify the selection criteria details. After you finish using these panels, you might also be prompted to provide additional information about the output and run option settings.
6. After you submit the job, the query results are sent to either an ISPF display panel or a printed report, depending on the output and run options you selected.

   For online results, you can use line commands to review the results. See "Using line commands on SMF data report result panels" on page 563.

Related topics

"Specifying advanced selection criteria for SMF records"

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Specifying advanced selection criteria for SMF records

You can further qualify the selection criteria for SMF records using the Advanced selection criteria options available on the Events selection panels. The advanced options available depend on the type of report you are generating. When you select multiple options, the panels for specifying the criteria are presented in sequence before the query is processed.

1. Type / in the input field for the advanced selection criteria you want to specify.
2. Press **Enter**.
3. For each advanced criteria option you selected, use the panels that open to specify the criteria.
4. Press **Enter** to process the query.

Figure 428 on page 553 shows the advanced selection criteria options available for User Event reporting. Table 257 on page 553 describes the advanced selection criteria available for SMF records.

```
 Menu         Options       Info    Commands     Setup
_____________________________________________________________________________

                IBM Security zSecure Admin - Events - User Selection
Command ===> _____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Userid  . . . . . _________     (userid or EGN mask)
Owned by  . . . . . _________     (group or userid, or EGN mask)
System  . . . . . ____          (system name or EGN mask)
Name  . . . . . ________________________ (name/part of name, no filter)
Installation data . ________________________ (scan of data, no filter)
Jobname . . . . . _________     (job name or EGN mask)
Terminal  . . . . . _________     (Terminal id or EGN mask)

Advanced selection criteria
_  User actions            _  User attributes         _  Date and time
_  Data set selection      _  HFS selection           _  Resource selection
_  DB2 selection           _  CICS selection          _  Omegamon selection
Output/run options
_  Include detail          _  Summarize              _  Specify scope
_  Output in print format  _  Customize title        _  Send as email
   _ Run in background     _  Sort differently
```

Figure 428. Events - User Selection panel

Table 257 describes the advanced selection criteria available for SMF records and provides references to additional information for each type.

Table 257. SMF records - Advanced Selection criteria

Advanced Criteria option	**Can be specified for these types of SMF information**	**For details, see ...**
User actions	User events, Group events	"Advanced selection criteria: User actions" on page 554
Group actions	Group events, Group events	"Advanced selection criteria: Group actions" on page 555
User attributes	User events	"Advanced selection criteria: User attributes" on page 555
Date and time	User events, Group events, Data set, Resource, Filesystem, IP selection, DB2	"Advanced selection criteria: Date and time" on page 556
Data set selection Further data set selection	User events, Group events, Data set	"Advanced selection criteria: (Further) Data set selection" on page 556
HFS selection	User events, Group events	"Advanced selection criteria: (Further) HFS selection" on page 557
Further pathname selection	Filesystem events	"Advanced selection criteria: (Further) pathname selection" on page 558
Resource selection Further resource selection	User events, Group events, Resource events	"Advanced selection criteria: (Further) Resource selection" on page 558
DB2 selection	User events, DB2 events	"Reporting on DB2 EVENTS (EV.4)" on page 570
DB2 user selection	DB2 events	"Advanced selection criteria: DB2 User selection" on page 559
DB2 object selection	DB2 events	"Advanced selection criteria: DB2 Object selection" on page 560

Table 257. SMF records - Advanced Selection criteria (continued)

Advanced Criteria option	Can be specified for these types of SMF information	For details, see ...
DB2 event selection	DB2 events	"Advanced selection criteria: DB2 Event selection" on page 560
IP selection Further IP selection	IP selection	"Advanced selection criteria: (Further) IP selection" on page 559
CICS selection Further CICS selection	CICS selection	"Advanced selection criteria: (Further) CICS selection" on page 561
Omegamon selection	Omegamon selection	"Advanced selection criteria: Omegamon selection" on page 561

Advanced selection criteria: User actions: Use this advanced selection criteria option to further qualify the SMF record selection based on actions performed by the user IDs specified in the selection criteria. When you select the **User actions** option on the record selection panel, the panel shown in Figure 429 opens to specify the selection criteria.

For details on setting up and running SMF queries, see "Querying SMF data" on page 551.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Events - User Action Selection
Command ===> ________________________________________________________________________
SMF records for all users
Show user related information

Logon/logoff/job start/job end
_  Successful                          _  Failed

Other user activity
_  Revoke/resume activity
_  RACF/CKGRACF commands issued
  _  Successful                        _  Failed
    _  Select command type(s)
  _  Include SETROPTS REFRESH/LIST commands
  _  Include ALTUSER RESUME commands
  _  Include CKGRACF commands
_  Affected by RACF/CKGRACF commands
```

Figure 429. Events - User Action Selection panel

All selections on this screen share an *or* relationship. As a result, selecting additional options increases the number of SMF records selected. Use field sensitive help for a description of the selection fields on this panel.

If you check the **RACF/CKGRACF commands issued** option and the **Select command type(s)** option on the selection panel, then the panel shown in Figure 430 on page 555 opens to specify the selection criteria.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - User Command Selection
Command ===> ____________________________________________________________________
SMF records for all users
RACF commands
 _  ADDUSER      _  ADDSD        _  ADDGROUP     _  RDEFINE
 _  ALTUSER      _  ALTDSD       _  ALTGROUP     _  RALTER
 _  DELUSER      _  DELDSD       _  DELGROUP     _  RDELETE
 _  PASSWORD     _  PERMIT       _  CONNECT      _  SETROPTS
 _  RACLINK      _  RVARY        _  REMOVE       _  RACDCERT
 _  RACPRIV

Unix commands
 _  chmod        _  chown        _  chaudit      _  setfacl
```

Figure 430. Events - User Command Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: Group actions: Use this option to select records based on actions performed by the group IDs that you are interested in. When you check the **Group actions** option on the selection panel, the panel shown in Figure 431 opens to specify the selection criteria.

For detailed field information, position your cursor in the field selection area and press F1 to view the online help.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events -  Group Action Selection
Command ===> ____________________________________________________________________

Show group related information

 _  Affected by RACF/CKGRACF commands
```

Figure 431. Events - Group Action Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: User attributes: Use this option to select SMF records based on attributes of the user IDs that you are interested in. When you check the **User attributes** option on the selection panel, the panel shown in Figure 432 on page 556 opens to specify the criteria.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - User Attribute selection
Command ===> ____________________________________________________________________
SMF records for all users
Show user related information

User attributes from SMF
OR_    _   Special       _   Operations    _   Auditor      _   Trusted
       _   Undefined     _   Audited



User attributes in RACF
OR_    _   Special       _   Operations    _   Auditor
```

Figure 432. Events - User Attribute Selection panel

The User attributes from SMF and User attributes in RACF selections are ANDed in the generated CARLa query.

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: Date and time: Use this option to select SMF records based on the date and time ranges during which the events you are interested in were performed. When you check the **Date and time** option on the selection panel, the panel shown in Figure 433 opens to specify the criteria.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Date selection
Command ===> ____________________________________________________________________
SMF records for all users
Include SMF records that fit any of the following criteria

                   From         Until          <     Calendar     >
Time               ____       : ____               August 2000
Date               __________ : __________     Mo Tu We Th Fr Sa Su
Weekday            ___        : ___                 1  2  3  4  5  6
                                                  7  8  9 10 11 12 13
                                                 14 15 16 17 18 19 20
                                                 21 22 23 24 25 26 27
                                                 28 29 30 31
```

Figure 433. Events - Date Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: (Further) Data set selection: Use this option to select SMF records based on the data sets you specify. When you check the **(Further) Data set selection** option, the panel shown in Figure 434 on page 557 opens to specify the criteria.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Dataset Selection
Command ===> ____________________________________________________________________
SMF records for all users
Dataset selection criteria (Dataset name or EGN mask)
_____________________________________________________________________________
_____________________________________________________________________________

Dataset exclusion criteria (Dataset name or EGN mask)
_____________________________________________________________________________
_____________________________________________________________________________

  _  Exclude temporary data set access
  _  Exclude access to user data sets
  _  Exclude online access to ISPF and Security zSecure data sets
  _  Resolve VSAM naming issues (full CKFREEZE file will be read)

Action on member  . _ Input  _ Output    _ Add    _ Delete    _ Rename    _ Replace
Level . . . . . .  __ __      (installation defined resource level)

RACF access intent at least                                    Result
_  1. Execute   2. Read                                        _  Success
   3. Update    4. Control                                     _  Violation
   5. Alter     6. All                                         _  Warning
```

Figure 434. Events - Data set Selection panel

To specify the exclusion and action criteria, type a / in each criteria field you want to use. For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: (Further) HFS selection: Use this option to select SMF records based on the UNIX files/directories you specify. When you check the **(Further) HFS selection** option on the selection panel, the panel shown in Figure 435 opens to specify the criteria.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Unix File/Dir. Selection
Command ===> ____________________________________________________________________
SMF records for all users                                rbl;
Pathname selection criteria (Pathname or EGN mask)
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________

Pathname exclusion criteria (Pathname or EGN mask)
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________

  _  Exclude files on TFS
  _  Resolve pathnames (full CKFREEZE file will be read)

Intended access                    Access used
_  Write                           _  Write
_  Read                            _  Read
_  Execute                         _  Execute
```

Figure 435. Events - Unix File Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: (Further) Resource selection: Use this option to select SMF records based on general resource profile characteristics such as class and resource name. When you check the **Resource selection** option on the selection panel, the panel shown in Figure 436 opens to specify the criteria.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Resource Selection
Command ===> ____________________________________________________________________
SMF records for all users
Resource selection criteria
Class     Resource name or EGN mask
________ ________________________________________________________________________
________ ________________________________________________________________________
________ ________________________________________________________________________

Resource exclusion criteria
Class     Resource name or EGN mask
________ ________________________________________________________________________
________ ________________________________________________________________________
________ ________________________________________________________________________

Level . . . . . __ __         (installation defined resource level)

Action against resource      Intended access at least       Result
_  Accessed  _  Updated      _  1. Execute   2. Read        _  Success
_  Added                        3. Update    4. Control     _  Violation
_  Deleted                      5. Alter     6. All         _  Warning
```

Figure 436. Events - Resource Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: (Further) pathname selection: This panel opens when you select the **Further pathname** selection option to select SMF records based on general resource profile characteristics such as class and resource name. When you check the **Resource selection** option on the selection panel, the panel shown in Figure 436 opens to specify the criteria.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - Resource Selection
Command ===> ____________________________________________________________________
SMF records for all users
Resource selection criteria
Class     Resource name or EGN mask
________ ____________________________________________________________________
________ ____________________________________________________________________
________ ____________________________________________________________________

Resource exclusion criteria
Class     Resource name or EGN mask
________ ____________________________________________________________________
________ ____________________________________________________________________
________ ____________________________________________________________________

Level . . . . . __ __         (installation defined resource level)

Action against resource      Intended access at least       Result
_  Accessed  _  Updated      _  1. Execute   2. Read        _  Success
_  Added                      3. Update    4. Control     _  Violation
_  Deleted                    5. Alter     6. All         _  Warning
```

Figure 437. Events - Resource Selection panel

For detailed field information, position your cursor in the field selection area. Then, press F1 to view the help.

Advanced selection criteria: (Further) IP selection: Use this option to select SMF records based on additional IP addresses and criteria relating to IP record types. When you check the **Further IP selection** option on the Event selection panel, the panel shown in Figure 438 opens to specify the criteria.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - IP selection
Command ===> ____________________________________________________________

IP address(es) to select (IP address or EGN mask)
________________________________________
________________________________________
________________________________________

IP address(es) to exclude (IP address or EGN mask)
________________________________________
________________________________________
________________________________________

Record types to include
_  FTP    _ Telnet   _  z/OS Firewall    _ HTTP logs (non-SMF)
```

Figure 438. Events - Further IP Selection panel

For detailed field information, position your cursor in the field selection area. Then, press F1 to view the help.

Related topic

"Querying SMF data" on page 551

Advanced selection criteria: DB2 User selection: Use this option to select SMF records based on the DB2 event criteria that you specify. When you check the **User selection** option on the DB2 selection panel, the panel shown in Figure 439 on page 560 opens to specify the criteria.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - DB2 Selection
Command ===> ____________________________________________________________________
SMF records for all DB2 events

Userid . . . . . ________     (userid or EGN mask)
Primary authid . . _____________________________________ (id or EGN mask)
Secondary authid . _____________________________________ (id or EGN mask)
SQLID  . . . . . . _____________________________________ (id or EGN mask)
Submitting id  . . _____________________________________ (id or EGN mask)
Remote client id . ____________________ (id or EGN mask)
Application userid ____________________ (id or EGN mask)
Role . . . . . . . ____________________ (role or EGN mask)
```

Figure 439. Events - DB2 User Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Advanced selection criteria: DB2 Object selection: Use this option to further qualify the selection of DB2-related SMF records based on the DB2 event criteria that you specify. When you check the **Object selection** option on the DB2 selection panel, the panel shown in Figure 440 opens to specify the criteria.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - DB2 Selection
Command ===> ____________________________________________________________________
SMF records for all DB2 events

Object name . _____________________________________ (name or EGN mask)
Plan  .  .  . ________ (name or EGN mask)

Enter "/" to specify object types to include
/  bufferpool    /  collection    /  database      /  distinct type
/  function      /  JAR           /  package       /  schema
/  procedure     /  plan          /  sequence      /  procedure
/  tablespace    /  storage group /  table         /  view
/  userauth      /  ACEE          /  row           /  trusted context
/  role
```

Figure 440. Events - DB2 Object Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topics

"Querying SMF data" on page 551

Advanced selection criteria: DB2 Event selection: Use this option to further qualify the selection of DB2-related SMF records based on the DB2 event criteria that you specify. When you check the **Event selection** option on the DB2 selection panel, the panel shown in Figure 441 on page 561 opens to specify the criteria.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - DB2 Selection
 Command ===> ____________________________________________________________________
SMF records for all DB2 events

Event types
1  1. Show all DB2 events
   2. Only select security related events
   3. Only select violations

Suppress IFCIDs (separated by commas)
_______________________________________________________________________________
```

Figure 441. Events - DB2 Event Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topics

"Querying SMF data" on page 551

Advanced selection criteria: (Further) CICS selection: Use this option to further qualify the selection of CICS-related SMF records based on user, transaction, and network selection criteria. When you check the **Further CICS selection** option on the CICS selection panel, the panel shown in Figure 442 opens to specify the criteria.

```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - CICS selection
Command ===> ____________________________________________________________________
SMF records for all CICS monitor records

User selection
Userid              ________       (userid or EGN mask)
User name           ___________________________________
Transaction selection
Transaction name    ____       (transaction or EGN mask)
Transaction type    _ Terminal input           _  ATI with data     _  ATI w/o data
                    _  User request            _  TCTTE trans.id           _  FEPI
                    _  Transient data trigger
CICS tran abended   _ (Y/N)
Network selection
Cics terminal name  ____             (terminal or EGN mask)
LU name             ________     (luname or EGN mask)
Network name        ________     (network or EGN mask)
Remote network      _                  (Y/N/blank)
```

Figure 442. Events - Further CICS Selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topics

"Querying SMF data" on page 551

Advanced selection criteria: Omegamon selection: Use this option to further qualify the selection of Omegamon-related SMF records based on user, transaction, and network selection criteria. When you check the **Omegamon selection** option on the User selection panel, the panel shown in Figure 443 on page 562 opens to specify the criteria.

```
 Menu         Options       Info    Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
              zSecure Admin+Audit for RACF - Events - Omegamon Selection
Command ===> ____________________________________________________________________

Show records that fit all of the following criteria:
Command name  . . . _________      (command name or EGN mask)
Command results . .    1. Allowed    2. Denied     3. All
Omegamon jobname  . ________       (jobname or EGN mask)
```

Figure 443. Events - Omegamon selection panel

For detailed field descriptions, position your cursor in the field selection area. Then, press F1 to view the help.

Related topics

"Querying SMF data" on page 551

Selecting Output/run options

Use the **Output/run options** to control how your query is run and the format of the generated output.

The **Output/run options** settings you specify on any of the Events panels are saved in your ISPF profile. They become the default settings for all Event panels that provide the option. For example, if you select the **Output in print format** option that option becomes the default setting on all the other Event panels that include that option. Some options require further configuration before running the query. The program provides configuration panels for these options after you select them.

To specify the output and run options for a query, do the following:

1. To change the default setting on a panel, remove the selection from the field.
2. For each option you require, type a / in the selection field for the option.
3. Press **Enter**.
4. Specify any further configuration for each option on the subsequent panels that open. Only some options require further configuration. The program prompts you for the information when required.

   If you select multiple options, any configuration panels for the options are presented in sequence until all required output and run parameters are specified.
5. Press **Enter** to run the query. (See "Querying SMF data" on page 551.)

Table 258 describes the available output and run options.

Table 258. Output and run options for

Output/Run option	Description
Include detail	Check this option to create a detailed report or display rather than the default one line per event summary display. If you have selected **Output in print format**, the report has between two and four output lines for each event. If an ISPF display is generated, each event has its own detail display. This option cannot be used in combination with the **Summarize** option.

Table 258. Output and run options for (continued)

Output/Run option	Description
Summarize	Check this option to creates a summary report or display with a one line summary of each SMF record. This option cannot be used in combination with the **Include detail** option.
Specify scope	Check this option to limit the output to the scope of a user ID or group, that is only the resources to which the specified user or group has direct or indirect access are reported.
Output in print format	Check this option to generate a printable report. When this option is selected, you can also use the options to customize the report title and send the report using email.
Customize title	Change the default report title. This option is only available when the **Output in print format** option is selected.
Send as email	If **Output in print format** is selected, you can select this option to send the report using email. A panel opens for specifying the email address destination for the report. The email function does not work until you have configured the SMTP options with `SETUP OUTPUT`. See "SE.7 Setup - Output" on page 1665.

Using line commands on SMF data report result panels

On the results panel for SMF queries, you can use line commands on the overview and detail display. Commands can be generated by issuing a line command at the start of a line. Line commands on both the overview and detail displays depend on the type of field that is shown.

Line commands on overview displays: Table 259 list the commands available for SMF records containing RACF data set profile information. Some of these actions might not be available to you because of the installed product combination, system specifications, or authorization.

When you use the / line command to verify which line commands are permitted, the following table is shown.

Table 259. Line commands on overview displays - RACF data set profiles

Command	Meaning	Explanation
C	Copy data set profile	C - Copy "Line commands" on page 54
D	Delete data set profile	D - Delete "Line commands" on page 54
L	List profile	The output of the `listdsd` command is presented in a browse panel.
P	Display data set profile	"Dataset profile detail display" on page 140
S	Show additional information	S - Select "Line commands" on page 54

Line commands on detail displays: Line commands on detail displays depend on the type of field that is shown. Table 260 on page 564 shows a list of the available commands. To include the detail information in the output, select the **Include**

detail option from the **Output/Run options** field group on the selection panels. See "Selecting Output/run options" on page 562.

Table 260. Line commands available on detail displays

Command	Meaning	Explanation
B	Browse data set	Only available for the data set field. This command browses the selected data set using the ISPF BROWSE service.
L	List profile	Only available for fields containing RACF profile information, user ID for example. The output of the list command is presented in a browse panel.
N	NSLOOKUP	Only available for TCP/IP and Firewall fields containing IP address information. The NSLOOKUP command queries a domain name server for information about a host or domain. This command can be interrupted with ATTN.
P	PING	Only available for TCP/IP and Firewall fields containing IP address information. The PING command sends an echo request to a node to determine whether the computer is accessible. When a response is received, the elapsed time is shown. Otherwise, a timeout message shows after a few seconds. This command can be interrupted with ATTN.
T	TRACERTE	Only available for TCP/IP and Firewall fields containing IP address information. The TRACERTE command sends UDP requests with varying TTL (time-to-live) values and then waits for the routers between the local and remote hosts to send TTL-exceeded messages. This command can be interrupted with ATTN.

Reporting on user events (EV.U)

The User Events panels are designed to select and show SMF audit trail records related to actions performed by users. SMF records that do not relate to something that was performed under the authority of a user ID are not selected. For example, records related to system events such as an IPL are not selected, but the commands issued by a user might be.

To specify selection criteria and generate the report, type **EV.U** on the command line to open the selection panel shown in Figure 444 on page 565.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - User Selection
Command ===>_____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Userid  . . . . . C##QAO__     (userid or EGN mask)
Owned by  . . . . . ________    (group or userid, or EGN mask)
System  . . . . . ____         (system name or EGN mask)
Name  . . . . . _____________________________ (name/part of name, no filter)
Installation data . _____________________________ (scan of data, no filter)
Jobname . . . . . ________     (job name or EGN mask)
Terminal  . . . . . ________    (Terminal id or EGN mast)

Advanced selection criteria
_  User actions          _  User attributes         _  Date and time
_  Data set selection    _  HFS selection           _  Resource selection
_  DB2 selection         _  CICS selection           _  Omegamon selection
Output/run options
_  Include detail          _  Summarize               _  Specify scope
_  Output in print format  _  Customize title         _  Send as email
  _  Run in background     _  Sort differently
```

Figure 444. Events - User Selection panel

If the selection panel is left blank, all data set related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: User actions" on page 554

– "Advanced selection criteria: User attributes" on page 555

– "Advanced selection criteria: Group actions" on page 555

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) Data set selection" on page 556

– "Advanced selection criteria: (Further) HFS selection" on page 557

– "Advanced selection criteria: (Further) Resource selection" on page 558

– "Reporting on DB2 EVENTS (EV.4)" on page 570

– "Reporting on CICS monitoring events (EV.5)" on page 571

– "Reporting on Omegamon events (EV.6)" on page 572

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on group events (EV.G)

The Group Events panels are designed to select SMF audit trail records related to actions performed by users of a specific group. If the SMF record does not relate to something that was performed under the authority of a user ID logged on using the group, it is not selected. For example, records related to system events such as an IPL are not selected, but the commands issued by a user might be.

To specify selection criteria and generate the report, type **EV.G** on the command line to open the selection panel shown in Figure 445.

```
  Menu   Options   Info   Commands   Setup
 ------------------------------------------------------------------------------
                        zSecure Suite - Events - Group Selection
Command ===> ____________________________________________________   _ start panel

 Show records that fit all of the following criteria:
 Group . . . . . . . C##QAO__     (group profile key or EGN mask)
 Owned by  . . . . . ________     (group or userid, or EGN mask)
 System  . . . . . . ____         (system name or EGN mask)
 Installation data . ________________________ (scan of data, no filter)
 Jobname . . . . . . ________     (job name or EGN mask)
 Terminal. . . . . . ________     (terminal id or EGN mask)

 Advanced selection criteria
 _  User actions          _  Group actions          _  Date and time
 _  Data set selection    _  HFS selection          _  Resource selection

 Output/run options
 _  Include detail        _  Summarize              _  Specify scope
 _  Output in print format _  Customize title       _  Send as email
   _  Run in background   _  Sort differently
```

Figure 445. Events - Group Selection panel

If the selection panel is left blank, all SMF records that have a group ID in them are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields. For example, you can select all SMF records that relate to actions performed by users connected to a group that have the characters `C##QAO` in the first six positions by typing `C##QAO*` in the group field.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: User actions" on page 554

– "Advanced selection criteria: Group actions" on page 555

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) Data set selection" on page 556

– "Advanced selection criteria: (Further) HFS selection" on page 557

– "Advanced selection criteria: (Further) Resource selection" on page 558

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on data set events (EV.D)

The Data set Events panels are designed to select SMF audit trail records related to actions involving data sets. If the SMF record does not relate to a data set, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user is not selected.

To specify selection criteria and generate the report, type **EV.D** on the command line to open the selection panel shown in Figure 446 on page 567.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Data set Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Data set name . . . ____________________________________________
Data set member . . ________     (member name or EGN mask)
Dataset profile . . ____________________________________________
System  . . . . . . ____         (system name or EGN mask)

Advanced selection criteria
_  Date and time         _  Further data set selection

Action on member  . _ Input  _ Output    _ Add    _ Delete    _ Rename    _ Replace
Level . . . . . . . __ __      (installation defined resource level)

Output/run options
_  Include detail          _  Summarize              _  Specify scope
_  Output in print format  _  Customize title        _  Send as email
  _  Run in background     _  Sort differently
```

Figure 446. Events - Data set Selection panel

If the selection panel is left blank, all data set related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) Data set selection" on page 556

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on general resource events (EV.R)

The Resource Events panels are designed to select SMF audit trail records related to actions involving resources. If the SMF record does not relate to a resource, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected.

To specify the selection criteria and generate the report, type **EV.R** to open the selection panel shown in Figure 447 on page 568.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - Resource Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Resource  . . . . . ________________________________________________________
Class . . . . . ________     (class or EGN mask)
Profile . . . . . ________________________________________________________
System  . . . . . ____       (system name or EGN mask)

Advanced selection criteria
_  Date and time         _  Further resource selection

Output/run options
_  Include detail        _  Summarize              _  Specify scope
_  Output in print format _  Customize title       _  Send as email
  _  Run in background   _  Sort differently
```

Figure 447. Events - Resource Selection panel

If the selection panel is left blank, all resource-related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) Resource selection" on page 558

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on Unix file system events from SMF and other logs (EV.F)

The Events - Filesystem Selection panels are designed to select and report on SMF audit trail records related to actions performed on Unix files or directories. If the SMF record does not relate to a Unix file or directory, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected. Records from selected HTTP access and error logs might also be present.

To specify selection criteria and generate the report, type **EV.F** on the command line to open the selection panel shown in Figure 448 on page 569.

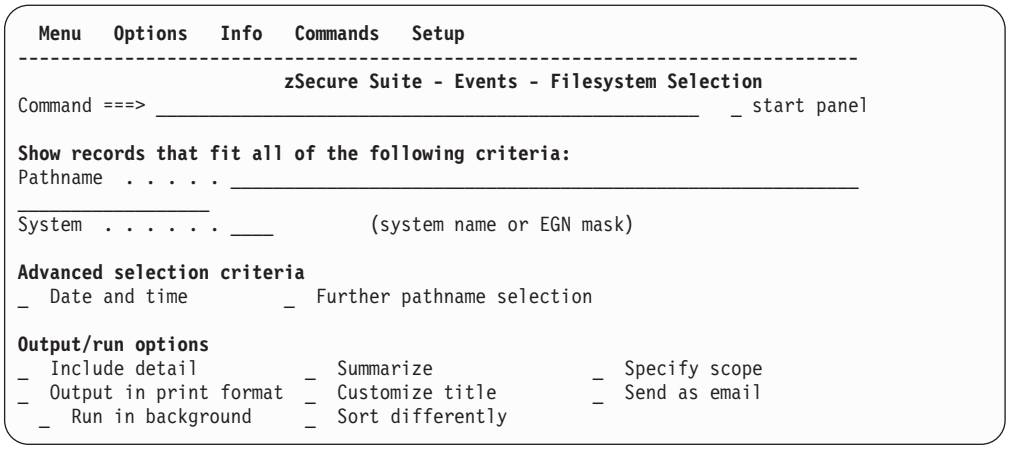


Figure 448. Events - Filesystem Selection panel

If the selection panel is left blank, all SMF records related to the file system are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) Resource selection" on page 558

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on IP events from SMF and other logs (EV.I)

The IP Events panels are designed to select SMF audit trail records containing IP addresses. If the SMF record does not relate to an IP address, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected.

To specify the selection criteria and generate the report, type **EV.I** to open the selection panel shown in Figure 449 on page 570.

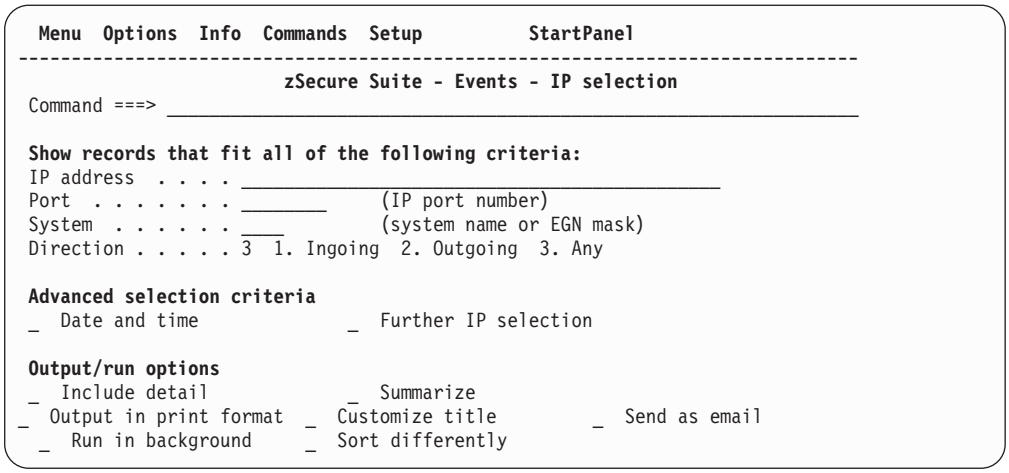


Figure 449. Events - IP Selection panel

If the selection panel is left blank, all IP related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For detailed field information, press F1 on the selection panel or any field to open the help.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: (Further) IP selection" on page 559

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on DB2 EVENTS (EV.4)

The DB2 Events panels are designed to select SMF audit trail records related to actions pertaining to DB2. If the SMF record does not relate to DB2, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected.

To specify selection criteria and generate the report, type **EV.4** on the command line to open the selection panel shown in Figure 450 on page 571.

```
   Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - DB2 Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
DB2 subsystem . . . ____         (subsystem name or EGN mask)
System  . . . . . . ____         (system name or EGN mask)

Advanced selection criteria
_  User selection          _  Object selection        _  Date and time
_  Event selection

Output/run options
/  Include detail          _  Summarize
_  Output in print format  _  Customize title         _  Send as email
  _  Run in background     _  Sort differently
```

Figure 450. Events - DB2 selection panel

If the selection panel is left blank, all DB2-related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For additional information, press F1 to open the online help for this panel or a specific field on the panel.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: DB2 User selection" on page 559

– "Advanced selection criteria: DB2 Object selection" on page 560

– "Advanced selection criteria: Date and time" on page 556

– "Advanced selection criteria: DB2 Event selection" on page 560

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on CICS monitoring events (EV.5)

The CICS Events panels are designed to select SMF audit trail records related to actions pertaining to CICS monitoring information. If the SMF record does not relate to a CICS transaction, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected.

To specify selection criteria and generate the report, type **EV.5** on the command line to open the selection panel shown in Figure 451 on page 572.

```
   Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - CICS Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following citeria:

Application name .  ________   (application name or EGN mask)
CICS specific APPL  ________   (application name or EGN mask)
CICS jobname  . . . ________   (jobname or EGN mask)
System  . . . . . .  ____          (system name or EGN mask)

Advanced selection criteria
/  Further selection             _ Date and time

Output/run options
/  Include detail
_  Output in print format  _  Customize title         _  Send as email
  _  Run in background     _  Sort differently
```

Figure 451. Events - CICS selection panel

If the selection panel is left blank, all CICS-related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For additional information, press F1 to open the online help for this panel or a specific field on the panel.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: (Further) CICS selection" on page 561

– "Advanced selection criteria: Date and time" on page 556

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Reporting on Omegamon events (EV.6)

The Omegamon Events panels are designed to select SMF audit trail records related to Omegamon commands. If the SMF record does not relate to an Omegamon command, it is not selected. For example, records related to system events such as an IPL or MVS commands issued by a user are not selected.

To specify selection criteria and generate the report, type **EV.6** on the command line to open the selection panel shown in Figure 452 on page 573.

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Events - Omegamon Selection
Command ===> ____________________________________________________   _ start panel

Show records that fit all of the following criteria:
Command name  . . . _________     (command name or EGN mask)
Command results . .    1. Allowed    2. Denied     3. All
Omegamon jobname  . ________      (jobname or EGN mask)
System  . . . . . . ____         (system name or EGN mask)

Advanced selection criteria
_  Date and time

Output/run options
_  Include detail          _  Summarize               _  Specify scope
/  Output in print format  _  Customize title         _  Send as email
  _  Run in background     _  Sort differently
```

Figure 452. Events - Omegamon selection panel

If the selection panel is left blank, all Omegamon-related SMF records are selected. You can limit the SMF records selected by filling one or more fields to be used as selection criteria. Only records that match all criteria are selected. Filters can be used in some of the selection fields.

For additional information, press F1 to open the online help for this panel or a specific field on the panel.

Related topics

"Querying SMF data" on page 551

"Specifying advanced selection criteria for SMF records" on page 552

– "Advanced selection criteria: (Further) CICS selection" on page 561

– "Advanced selection criteria: Date and time" on page 556

"Selecting Output/run options" on page 562

"Using line commands on SMF data report result panels" on page 563

Using the predefined RACF event analysis reports (SMF Reports)

Use EVENTS menu option **1** SMF REPORTS to run predefined RACF event analysis reports.

To select and run the reports, type EV.1 on the command line to open the SMF report menu shown in Figure 453.

```
 Menu   Options   Info   Commands   Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Events - SMF reports
Command ===> ____________________________________________________________

1    Exceptions      RACF exception report
2    Stat hour       RACF statistics by hour (very wide report)
3    Stat time       RACF statistics by time
4    Stat day        RACF statistics by weekday
5    Revoke/resume   RACF revoke/resume summary
9    Job viols       Dataset violations by batch jobs
A    APPC conv       APPC conversation summary
```

Figure 453. Events SMF reports menu

Table 261 describes the available report options.

Table 261. Predefined SMF Analysis report options

1 Exceptions	Create a group of reports showing all RACF exceptions; both DETAIL and LIST formats are supported. The layout of each report type is dependent on the RACF event type described. No select or exclude parameters can be specified with this report.
2 Stat hour	Show RACF: statistics by hour, in a wide layout (180 positions).
3 Stat time	Show RACF statistics by hour, in a layout fitting into 80 positions.
4 Stat day	Show RACF statistics by weekday, in a layout fitting into 80 positions. Use this option with SMF data for several days. If you use live SMF data, the report only includes all events that occrred on one day (today).
5 Revoke/Resume	Show RACF revoke and resume command activity summarized in two ways: by target user ID and by administrator.
9 Job viols	Show batch jobs and started tasks that have data set security violations.
A APPC conv	Show APPC conversations summarized in 4 ways: by local LU name, by partner LU name, by local RACF group, and by local user ID and descending frequency.

For most report types, after you select the report option, a series of panels are shown so you can specify additional select, exclude, and report parameter panels. These panels are described in "Generating pre-defined SMF and RACF event reports" on page 579.

For more information on reports and report examples, see the following topics:

- "RACF Exceptions report example"
- "RACF statistics report example" on page 576

RACF Exceptions report example

The RACF Exceptions report provides a list of all RACF exceptions logged. This example starts with the RACF Exceptions report overview which organizes RACF events into different report types. The overview is followed by samples of the detail information you can access from the overview panel.

After you run an **Exceptions** report, a selection panel shows the RACF events ordered into different report types. The report overview panel shown in Figure 454 on page 575 opens.

```
zSecure Audit Display Selection                    11 s elapsed, 4.8 s CPU
Command ===> _____________________________________________ Scroll ===> CSR

   Name         Rows Summary Records Title
_ USEOPER       1       2 Use of OPERATIONS Attribute
_ USESPEC       0       0 Use of SPECIAL Attribute
_ CMDSPEC       1       3 Commands issued by SPECIAL users
_ CMDFAIL       1       1 Command violations
_ AUDUSER       0       0 Auditing of Users
s DSETVIOL      6       7 Data set Access Violations by Profile and User
_ GRESVIOL      1       2 General Resource Access Violations by Class, Profile
_ UNIXVIOL      0       0 UNIX File Access Violations by Path and User
_ DSETWARN      0       0 Data set Access Warnings by Profile and User
_ GRESWARN      0       0 General Resource Access Warnings by Class, Profile a
_ VWBYUSER      1       8 Violations and Warnings by User
_ UNDEF         0       0 Access by Undefined Users
_ LOGTERM       1       2 Attempted Logon by Pwd/Userid Guessing, > 5 per Term
_ LOGUSER       0       0 Attempted Logon by Password Guessing, > 5 per Userid
_ LOGMANY       0       0 Too many Attempted Logons, User Revoked
_ LOGREVK       0       0 Attempted Logon by Revoked User
_ LOGATTN       0       0 Attempted Logon, attention required
_ KERBERR       0       0 Kerberos KDC errors
_ CA7VIOL       0       0 CA7 Logon Violations
_ CA7XSEC       0       0 CA7 External Security Activity
_ LOGF_L_F      0       0 Logon failures per logonid - frequent
******************************** BOTTOM OF DATA ********************************
```

Figure 454. RACF exception report overview panel

Select any report to view an event summary. In this example, the user selected the DSETVIOL the Data set Violations by Profile and User report which opens a panel that summarizes the data set profiles and violation as shown in Figure 455.

```
Dataset Access Violations by Profile and User                    Line 1 of 6
Command ===> _____________________________________________ Scroll===> CSR
                                          2Sep93 01:30 to  3Sep93 05:30
   Profile                               Users Count
__ B#AD.TELF.**                              1     1
__ C##S.GEMS2T.*.**                          1     1
__ R##PROX.*.**                              1     1
s_ C##A.D.C##BJTI.**                         1     2
__ SYS2.R##S.PROCLIB                         1     1
__ T##F0D.IPAFAS.*                           1     1
******************************** BOTTOM OF DATA ********************************
```

Figure 455. RACF Exceptions report - Dataset Access Violations by Profile and User

From this panel, you can select profiles to drill down to detailed information about the violations by profile and for individual users. Figure 456 on page 576 shows the detail view for a violation by profile ID and user ID.

```
Data Set Access Violations by Profile and User                  Line 1 of 36
Command ===> _____________________________________________ Scroll===> CSR
                                          2Sep93 01:30 to  3Sep93 05:30

  Description
  RACF ACCESS violation for C##BDV2: (UPDATE,READ) on DATASET C##A.D.C##JTI.ASM

  Record identification
  Job name + id                 C##BDV2
  SMF date/time                 Thursday   2 Sep 1993 12:11:43.50
  System ID                     DINO       record no: CNR5SM00 30138

  Event identification
  RACF event description        Resource access (Failure:Insufficient
  RACF event description        authority)
  RACF event qualifier          1
  RACF descriptor for event     Violation
  RACF reason for logging       Resource
  SAF authority used            Normal
  Access intent                 UPDATE
  Access allowed                READ
  Audit/message logstring

  Object identification
  SAF profile class             DATASET
  SAF profile key               C##A.D.C##JTI.**
_ SAF resource name             C##A.D.C##JTI.ASM
  Volume serial                 SM3001
  Resource token

  Object ownership
  Profile owner id              C##AINT
  Installation data

  Subject identification
_ User:  C##BDV2      Group: C##B         Terminal: TCDINO10   Appl:
  Name:  DAVE VITTORI                     Security label:
  Token: User:C##BDV2; Group:C##B; Flags:(Pre 1.9); Session:TSO;
  Token: Port:TERMINAL(TCDINO10)
****************************** BOTTOM OF DATA ********************************
```

Figure 456. RACF data set event display

Note: The other exception reports have different layouts, fitting the type of exception recorded.

RACF statistics report example

The STATISTICS reports show a simple summary of RACF events by hour or over time. You can specify selection and exclusion criteria using the normal select and exclude panels described in "Generating pre-defined SMF and RACF event reports" on page 579.

Figure 457 on page 577 shows the statistics over time report results generated by selecting the **Stat time** option from the SMF reports menu.

```
 BROWSE - C##BCO1.C2R1EF2A.REPORT                      LINE 000 13.3 s CPU, RC=8
 COMMAND ===> _____________________________________________ SCROLL ===> CSR
******************************** Top of Data *********************************
S M F   R E C O R D   L I S T I N G   20Jul98 07:00 to 27Jul98 06:30
Summary of RACF events by time of day

Event    Dsc SAF auth      00-08  08-12  12-18  18-24   total  %
RACINIT  S                    0      0      4      0       4  0
RACINIT  V                    0     19     27      1      47  0
ACCESS   S   N              995    794   2744    711    5244 49
ACCESS   V   N                4      1     36     14      55  0
DELETE   S   N                0      0      1      0       1  0
DEFINE   S   N                0      0      3      1       4  0
DEFINE   V   N                0      2     10      0      12  0
ALTUSER  S    S               0      0      2      0       2  0
ALTUSER  S   N                0      0      1      0       1  0
PERMIT   S    S               0      0      1      0       1  0
RDEFINE  S    S               0      0      3      0       3  0
SETROPTS V                    0      0      3      0       3  0
GENERAL  S                    3     41    171      0     215  2
GENERAL  V                    0      3     14      0      17  0
FACCESS  V   N                0      0      3      0       3  0
CHDIR    S   N               39     53    230    102     424  4
INITOEDP S   N               27     23     56     80     186  1
INITOEDP V                    1      1      4      0       6  0
TERMOEDP S           Su       0      0     10      0      10  0
TERMOEDP S   N               50     71    390    111     622  5
LINK     S   N                0      4      0      0       4  0
MKDIR    S   N                0      0    947      0     947  8
OPENFILE S   N               21     53   1793     15    1882 17
RENAMEF  S   N               14      4     45      0      63  0
RMDIR    S   N                0      0      4      0       4  0
SETEUID  S           Su      26     31    117     42     216  2
SETEUID  S   N               26     31    114     42     213  2
UNLINK   S   N               21     43    264     11     339  3
CHKPRIV  V   N                0      0      8      0       8  0
******************************* Bottom of Data ********************************
```

Figure 457. RACF statistics by time of day

The **Dsc** and **SAF Auth** columns in this report describe the RACF descriptor and RACF authority used. Table 262 shows the descriptor values that can occur.

Table 262. RACF Descriptor values

Descriptor value	Meaning
S	Success
U	Undefined user
V	Violation
W	Warning

Table 263shows the RACF authority values that can occur.

Table 263. RACF authority values

SAF auth value	Meaning
A	Auditor
B	Bypasses-user id = *BYPASS*
F	Failsoft processing
N	Normal authority check
O	OPERATIONS attribute
S	SPECIAL attribute

Table 263. RACF authority values (continued)

SAF auth value	Meaning
Su	OpenEdition MVS superuser
Sy	OpenEdition MVS system function
T	Trusted/Privileged attribute
X	Installation exit processing

For details, see "SMF: SMF records" on page 1276.

Logging for specific RACF events (EV.2 - RACF EVENTS)

Use the menu option **2** RACF EVENTS to audit specific RACF event types. When you select this option, the panel shown in Figure 458 opens.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - RACF events
Command ===> ____________________________________________________________

Enter "/" to select report(s)
_  All events       Overview of all following RACF events (except IPL)
_  Logging          RACF logging of all events except RACINIT
_  Not normal       RACF access not due to normal profile access
_  Warnings         RACF access due to profiles in warning modes
_  Violations       RACF access violations
_  Commands         RACF command auditing
_  CKGRACF          zSecure Admin CKGRACF commands
_  IPL RACF         RACF initialization
```

Figure 458. RACF EVENTS panel

Table 264 describes the available RACF Event report options.

Table 264. Events menu - RACF Event report options

All events	Select all RACF processing records and summarize them by event and event qualifier. Use this option to view all records for any distinct event, all invalid new password attempts for example. This option is mutually exclusive with all other, more selective, options. It also requires the largest amount of CPU time and memory.
Logging	Select all logged RACF processing records except RACINIT records. The resulting report includes command usage, access checks, and class and user logging. Job starts and logon events are not included.
Not normal	Select all RACF processing records where an authority other than normal was used. (Normal is the default for most users.) The selected authority types are: Operations, Special, Exit, Auditor, Failsoft, Bypassed, and Trusted.
Warnings	Select all accesses due to profiles in warning mode. These accesses were permitted but caused a warning to be issued. Other warning events are not selected.
Violations	Select all access failures. Other violations (like failed logons) are not selected.
Commands	Select all logged commands. This option selects all SETROPTS and RVARY commands, all commands requiring AUDITOR authority, all commands requiring special authority (only if SETROPTS SAUDIT is in effect), all ADDSD and RDEFINE commands requiring operations authority (only if SETROPTS OPERAUDIT is in effect), all commands issued by audited users (due to ALTUSER UAUDIT), and all command violations (only if SETROPTS CMDVIOL is in effect).

Table 264. Events menu - RACF Event report options (continued)

CKGRACF	Select all records written by the CKGRACF authorized component of Tivoli zSecure Manager for RACF z/VM. Both EVENT=ACCESS and EVENT=GENERAL records are selected. For more information about CKGRACF and the SMF records it writes, see Chapter 14, "CKGRACF Command Language," on page 1499.
IPL RACF	Select all records written at start of RACF (during IPL processing). These records contains the SETROPTS settings in use.

After selecting the report types on this panel, the selection, exclusion, and processing options panels are shown so you can specify further selection criteria. Records that meet the any of the following conditions are selected:

- Record is selected only if it matches one of the selected RACF event types.
- Matches the additional selection criteria.
- Does not match any of the exclusion criteria.

For information about generating and reviewing the reports, see the following topics:

- "Generating pre-defined SMF and RACF event reports"
- "Reviewing the RACF event reports" on page 582

Generating pre-defined SMF and RACF event reports

The SMF report (**EV.1**) and the RACF events (**EV.2**) functions provide pre-defined report layouts to format the SMF and RACF event data generated from the specified selection and exclusion criteria. The process to set up and generate the SMF and RACF Event reports is similar.

1. Specify selection criteria if prompted.

   For some report types, you cannot specify selection or exclusion criteria because the report type already focuses on a targeted set of data. For these reports, the report processing and display options panel opens immediately so you can limit the processing to a specified number of records, specify whether to include SAF (System Authorization Facility) data, and specify display and output options.
2. Specify exclusion criteria if prompted.
3. Specify report processing, display and format options.
4. Press Enter to begin processing the selected data.
5. SMF processing can be interrupted by pressing the **ATTN** key. No more records are read, but processing continues.

   When you press this key, no more SMF records are read, but report processing continues. The resulting report includes information about the records that were processed before the ATTN key was pressed.
6. Review the report data on the display or in the printed report, depending on the options selected.

Related topics

- "Selecting event data" on page 580
- "Excluding event data" on page 580
- "Setting the report processing and display options" on page 581
- "Reviewing the RACF event reports" on page 582

Selecting event data

Use the Event selection panel to specify *selection* criteria to filter the report data. For each criteria you want to use, type a / , option number, or input value in the entry field, then press Enter for the next panel. Records are selected if the records fit *all* of the criteria specified on the panel.

After you enter the selection criteria, the Event exclusion panel opens so you can filter the selected records further.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Events - SMF selection
Command ===> ____________________________________________________________

Select SMF records that fit all of the following criteria
Use EGN masks for selection criteria
Userid  . . . . . ____________________________________________________________
Jobname . . . . . ____________________________________________________________
Terminal  . . . . ____________________________________________________________

Dataset name  . . . ____________________________________________________________

Profile class . . . ____________________________________________________________
Profile key . . . . ____________________________________________________________
Level . . . . . __   __      (installation defined resource level)

                    From         Until            Intended access at least
Time                ____       : ____             6  1. Execute  2. Read
Date                __________ : __________          3. Update   4. Control
Weekday             ___        : ___                 5. Alter    6. All access

Show all            _  Success   _  Warning   _  Violation
```

Figure 459. EVENTS selection menu

For detailed field descriptions, press F1 on the ISPF panel to view the help. The options selected on this panel are written to your ISPF profile and stored as the default values for the selection panel. If you change a selection, the default values are updated.

Excluding event data

After specifying selection criteria, the Event exclusion panel is open, so you can specify *exclusion* criteria. Records selected by the criteria specified on the preceding Event selection panel are excluded from the report if the records fit *any* of the criteria specified on this panel. The exclusion criteria are specified in the same way as the selection criteria. (See Figure 459.)

After pressing **Enter** on the selection panel, the *exclude* panel shown in Figure 460 on page 581 opens.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - SMF Exclusion
Command ===> ____________________________________________________________

Exclude SMF records that fit any of the following criteria
Use EGN masks for exclusion criteria
Userid  . . . . . ____________________________________________________
Jobname . . . . . ____________________________________________________
Terminal  . . . . ____________________________________________________

Dataset name  . . . SYSTCP.SMTP.**___________________________________________

Profile class . . . ____________________________________________________
Profile key . . . . ____________________________________________________

                    From         Until
Time                ____       : ____
Date                __________ : __________
Weekday             ___        : ___

Suppress all        _  Success   _  Warning   _  Violation
```

Figure 460. EVENTS exclusion menu

Note: The example shown in Figure 460 excludes all profiles matching the *filter* SYSTCP.SMTP.**. To exclude only the named profile (and not more specific profiles), enclose the profile in single or double quotation marks.

Setting the report processing and display options

After specifying the selection and exclusion criteria, the Events options panel shown in Figure 461 opens so you can specify report processing and display options. This panel opens for all SMF menus and is the last panel shown before report processing begins.

```
 Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - SMF options
Command ===> ____________________________________________________________

Input and output specifications
 Max number of SMF records to read  . . . ________   (default is no limit)
 Max number of records per display group  ________   (default is no limit)

 Complete with SAF data  1  1. Yes        2. No      3. Minimal

 _  Output in print format
 _  Use CKFREEZE data
 _  Show number of SMF records selected
 _  Run in background
```

Figure 461. EVENTS report parameters panel

For detailed field descriptions, press F1 on the ISPF panel to view the help. The options selected on this panel are written to your ISPF profile and stored as the default values for the selection panel. If you change a selection, the default values are updated.

After you specify the processing options and press Enter, report processing begins. During processing, data on the number security database record profiles, CKFREEZE records, and SMF records read is tracked. SMF processing can be interrupted by pressing the **ATTN** key. When you press this key, no more SMF records are read, but report data processing continues.

When processing is done, the report data is shown online or written to a report file depending on the options you selected. Written reports are generated through a batch job submitted in the background. Online reports open immediately after processing ends. For examples of the interactive reports, see "Reviewing the RACF event reports."

Reviewing the RACF event reports

RACF event reports can be sent to a printed report or an interactive online display. This topic describes the interactive reports. If you selected a printed report, you can review the report data in the file generated by the batch job that ran the report.

From the interactive RACF Event reports, you can view the following types of information:

- Summary of RACF record report data

  During processing, data on the number security database record profiles, CKFREEZE records, and SMF records read is tracked. If you select the **Show number of SMF records selected** processing option, this summary information can be viewed from the RACF Display Selection panel. (See Figure 462.)
- Summary of RACF event records by event type
- List of selected RACF records
- To view RACF records summarized by RACF event type, use the **All events** report option. From this view, you can drill down to view records by event type and details on individual events.
- The other reporting options output a list of all selected records without any summary information. From this view, you can drill down to view the event details for specific records. (See Figure 466 on page 585.)

Viewing summary of RACF event report data: During processing, data on the number security database record profiles, CKFREEZE records, and SMF records read is tracked. If you select the **Show number of SMF records selected** processing option, this summary information can be viewed from the RACF Display Selection panel shown in Figure 462.)

If you selected the **Show number of SMF records selected** option on the Event options panel (see Figure 461 on page 581), the Display Selection panel shown in Figure 462 is open to access a summary of the selected records. If you did not select that option, the list of selected records is opened on the SMF record RACF processing and audit records panel shown in Figure 464 on page 584.

```
zSecure Audit Display Selection                                  Line 1 of 2
Command ===> ____________________________________________________ Scroll===> CSR

  Name     Summary Records Title
_ SUMMARY       19    5730 SMF record summary table
_ RACFDATA    5730       0 SMF record RACF processing and audit records
****************************** BOTTOM OF DATA ********************************
```

Figure 462. EVENTS display overview

From this Display Selection panel, you can select the SUMMARY or RACFDATA:

SUMMARY
Selecting the SUMMARY option opens the SMF record summary table shown in Figure 463 on page 583 which lists the record type, subtype, number of selected records, and the relative frequency of SMF records fitting the selection

criteria.

```
SMF record summary table ---------------------------------------- Line 1 of 21
Command ===>                                                 Scroll===> CSR
                                                 22Sep94 15:15 to 22Sep94 16:15
Typ SubTp Records Freq
  2             1    0
  3             1    0
  4             7    5
  5             7    5
 20             7    5
 23             1    0
 26             6    4
 30     1       7    5
 30     2      16   11
 30     3       7    5
 30     4       7    5
 30     5       7    5
 30     6       8    5
 32     3       1    0
 40            20   14
 41             2    1
 60             4    2
 61             3    2
 80            25   17
 89     1       1    0
 90             1    0
****************************** BOTTOM OF DATA ******************************
```

Figure 463. EVENTS - Selected record summary

RACFDATA

Selecting the RACFDATA option opens the SMF record RACF processing and audit records panel. The information shown depends on what type of RACF event report you selected.

The *All events* reporting option provides a summary of selected records organized by RACF event type as shown inFigure 466 on page 585. The display also lists the numeric event qualifiers for each event type. This summary by RACF event type is only available for the *All events* reporting option.

All events reporting option

This option generates a summary view showing selected RACF event records organized by type as shown in Figure 464 on page 584. The display also lists the numeric event qualifiers for each event type.

```
SMF record RACF processing and audit records                    Line 1 of 25
Command ===> _____________________________________________ Scroll===> CSR
                                              15Jun08 15:11 to 11Mar10 01:32

   Event     Q      Count Event description
__ RACINIT   1         30 Racinit (Failure:Invalid password)
__ RACINIT   6          6 Racinit (Failure:Revoked userid attempting access)
__ RACINIT   7          3 Racinit (Failure:Userid automatically revoked)
__ RACINIT   9          2 Racinit (Failure:Undefined user id)
__ RACINIT  13          4 Racinit (Success:Successful racinit delete)
__ RACINIT  25          4 Racinit (Failure:Current password has expired)
__ ACCESS    0       3549 Resource access (Success:Successful access)
__ ACCESS    1         34 Resource access (Failure:Insufficient authority)
__ DEFINE    0          4 Define resource (Success:Successful definition)
__ DEFINE    3          1 Define resource (Failure:Insufficient authority)
__ DEFINE    6          1 Define resource (Failure:Resource not protected)
__ ALTUSER   0          3 Altuser command (Success:No violations detected)
__ PERMIT    0          1 Permit command (Success:No violations detected)
__ RDEFINE   0          3 Rdefine command (Success:No violations detected)
__ GENERAL   0        145 General auditing (Unclear:General audit record written)
__ CHDIR     0        158 Change directory (Success:Working directory changed)
__ INITOEDP  0         90 Init OMVS proc (Success:Successful process dub)
__ INITOEDP  1          4 Init OMVS proc (Failure:User not define to OMVS)
__ INITOEDP  3          1 Init OMVS proc (Failure:User current group has no GID)
__ TERMOEDP  0        224 Comp OMVS proc (Success:Process completed)
__ OPENFILE  0         85 Open new file (Success:File created)
__ RENAMEF   0         10 Rename file (Success:File renamed)
__ SETEUID   0        299 Set EUID (Success:Effective user-ID set)
__ UNLINK    0         73 Unlink file (Success:File was unlinked)
__ CHKPRIV   1          8 Check privilege (Success:User not authorized to function)
****************************** BOTTOM OF DATA ***********************************
```

Figure 464. SMF record RACF processing and audit records - summary by RACF Event type

To view information about a specific event type, select the Event type from the summary panel. Then, press Enter to view the list of event records for the specified event type as shown in Figure 465.

```
SMF record RACF processing and audit records              Line 1 of 2
Command input ===> _____________________________________ Scroll ===> CSR
                                          2Sep93 01:30 to  3Sep93 05:30
   Event     Q      Count Event description
   RACINIT  25          7 Racinit (Failure:Current password has expired)
   Date      Time  Description
__ 26Jun08 10:19:06.06 RACF RACINIT violation for CRMBFT1: Job Start / Logon
__ 01Jul08 13:15:43.81 RACF RACINIT violation for CRMBHJ1: Job Start / Logon
__ 21Aug08 11:19:31.80 RACF RACINIT violation for CRMBMVB: Job Start / Logon
__ 14Jan10 01:43:48.10 RACF RACINIT violation for CRMBBM1: Job Start / Logon
__ 18Jan10 13:59:19.77 RACF RACINIT violation for CRMQAP1: Job Start / Logon
__ 23Feb10 09:52:46.79 RACF RACINIT violation for CRMBCOLL: Job Start / Logon
__ 25Feb10 11:16:50.96 RACF RACINIT violation for CRMBDV1: Job Start / Logon

****************************** BOTTOM OF DATA ******************************
```

Figure 465. EVENTS overview of a single RACF event type

From this view, you can select individual records to view the event details. (See Figure 467 on page 586.)

Other report views

If you use a RACF event report option other than **All events**, the generated report lists the selected RACF records without a record type summary. Figure 466 on page 585 shows the list of selected RACF event records.

```
SMF record RACF processing and audit records                    Line 1 of 65
Command ===>                                                  Scroll===> CSR
                                                 20Jul98 13:18 to 26Jul98 00:35
   Date      Time  Description
__ 20Jul1998 13:18 RACF ACCESS violation for C##BTKR: (UPDATE,READ) on DATASET
__ 20Jul1998 13:18 RACF ACCESS violation for C##BTKR: (UPDATE,READ) on DATASET
__ 20Jul1998 13:19 RACF ACCESS violation for C##BTKR: (UPDATE,READ) on DATASET
__ 20Jul1998 13:22 RACF ACCESS violation for C##BTKR: (UPDATE,READ) on DATASET
__ 20Jul1998 16:57 RACF ACCESS violation for C##ASCH: (UPDATE,READ) on DATASET
__ 20Jul1998 16:57 RACF ACCESS violation for C##ASCH: (UPDATE,READ) on DATASET
__ 20Jul1998 16:59 RACF ACCESS violation for C##ASCH: (UPDATE,READ) on DATASET
__ 21Jul1998 15:39 RACF ACCESS violation for C##BHB2: (UPDATE,READ) on DATASET
__ 21Jul1998 20:01 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:01 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:02 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:02 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:05 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:05 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:06 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:06 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:13 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:13 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:20 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 21Jul1998 20:20 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 22Jul1998 10:58 RACF ACCESS violation for C##BLU1: (UPDATE,READ) on DATASET
s_ 22Jul1998 12:51 RACF ACCESS violation for C##AINT: (READ,NONE) on DATASET SY
__ 22Jul1998 12:52 RACF ACCESS violation for C##AINT: (UPDATE,READ) on FACILITY
__ 22Jul1998 12:52 RACF ALTUSER success for C##AINT: ALTUSER C##BHBE
__ 22Jul1998 12:53 RACF ALTUSER success for C##AINT: ALTUSER C##BHB2
__ 22Jul1998 16:16 RACF ACCESS violation for C##BOO2: (READ,NONE) on TSOPROC LI
__ 23Jul1998 12:26 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 23Jul1998 12:26 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 23Jul1998 12:49 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 23Jul1998 12:49 RACF ACCESS violation for C##BER2: (READ,NONE) on DATASET SY
__ 23Jul1998 13:18 RACF RDEFINE success for C##AROB: RDEFINE FACILITY AAA
__ 23Jul1998 13:19 RACF PERMIT success for C##AROB: PERMIT FACILITY AAA
__ 23Jul1998 13:21 RACF RDEFINE success for C##AROB: RDEFINE FACILITY AAA1
__ 23Jul1998 13:21 RACF RDEFINE success for C##AROB: RDEFINE FACILITY AAA2
__ 23Jul1998 14:39 RACF ALTUSER success for C##BTKR: ALTUSER C##BTKR
__ 23Jul1998 17:38 RACF ACCESS violation for C##AINT: (READ,NONE) on JESSPOOL D
__ 23Jul1998 17:38 RACF ACCESS violation for C##AINT: (READ,NONE) on JESSPOOL D
```

Figure 466. Overview of selected RACF event records

From the overview panel, select an event record to view the event details as shown in Figure 467 on page 586.

```
SMF record RACF processing and audit records                    Line 1 of 36
Command ===> _____________________________________________ Scroll===> CSR
                                          20Jul98 13:18 to 26Jul98 00:35


  Description
  RACF ACCESS violation for C##MAINT: (READ,NONE) on DATASET SYSAPPL.CNRACF.I
  OCONFIG

  Record identification
_ Jobname + id:  C##MAINT
  SMF date/time: Wed 22 Jul 1998 12:51:33.58
  SMF system:    DINO       record type:  80   record no: CNR1SM00 96250

  Event identification
  RACF event description        Resource access (Failure:Insufficient
  RACF event description        authority)
  RACF event qualifier          1
  RACF descriptor for event     Violation
  RACF reason for logging       Resource
  SAF authority used            Normal
  Access intent                 READ
  Access allowed                NONE
  Audit/message logstring

  Object identification
  SAF profile class             DATASET
  SAF profile key               SYSAPPL.CNRACF.**
_ SAF resource name             SYSAPPL.CNRACF.CKFREEZE
  Resource level                 0
  Volume serial                 SM3004
  Resource token

  Object ownership
_ Profile owner id              SYSPROG
  Installation data             SYSTEM PROGRAMMING

  Subject identification
_ User:  C##MAINT      Group: C##A        Terminal:            Appl:
  Name:  MAINTENANCE                      Security label:
  Token: User:C##MAINT; Group:C##A; Flags:(Pre 1.9); Session:STC
****************************** BOTTOM OF DATA ********************************
```

Figure 467. RACF event detail display

Creating custom queries and reports (EV.C CUSTOM)

Use the EVENTS menu option C CUSTOM to create custom queries and displays. This customization uses predefined detail layouts to generate queries. You can use this panel to phrase queries that do not fit the selection and exclusion panels provided on other SMF menus. You can also create queries using the COMMAND or LIBRARY options on the main menu.

The following examples show a custom query with a predefined layout followed by a custom query with a custom layout.

The display in Figure 468 on page 587 shows the first CUSTOM panel.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Custom
Command ===> ____________________________________________________________

newlist type  . . . . . SMF_____________________

Enter up to 3 SELECT condition sets (use EGN masks)
Select  user=CRMB*_____________________________________________________________
Select  _______________________________________________________________________
Select  _______________________________________________________________________

Enter up to 3 EXCLUDE condition sets (use EGN masks)
Exclude jobname=ifasmfdp_______________________________________________________
Exclude _______________________________________________________________________
Exclude _______________________________________________________________________

Enter up to 3 DEFINE commands
Define  _______________________________________________________________________
Define  _______________________________________________________________________
Define  _______________________________________________________________________
```

Figure 468. EVENTS CUSTOM query panel

- You can specify any SELECT and EXCLUDE clause on this panel.
- Use AND, OR, and NOT to combine clauses.
- Valid NEWLIST types are SMF and all DEFTYPEs defined in SE.U (see "SE.U SETUP - user-defined input sources" on page 1667).
- All the fields defined for the `NEWLIST` specified can be used (for `NEWLIST TYPE=SMF` see "SMF: SMF records" on page 1276 for a language reference).
- To be selected, a record must match any SELECT statement and none of the EXCLUDE statements. If no SELECT clause is specified, all records are selected (before EXCLUDE processing); if no EXCLUDE clause is specified, no records are excluded.
- You can also define boolean or statistic variables for a custom display. These variables or other user-defined fields cannot be used in the predefined layouts.

The selection panel is followed by the custom display panel in Figure 469 on page 588.

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Events - Custom
Command ===> ____________________________________________________________________

Enter output variables:
Display ____________________________________________________________________
        ____________________________________________________________________
        ____________________________________________________________________

Enter summary variables:
Summary ____________________________________________________________________
        ____________________________________________________________________
        ____________________________________________________________________

Or select one or more default reports:
_ RACF processing and audit                    _  CICS audit
s  Job activity                                 _  DB2 audit
s  Dataset activity                             _  Firewall activity
_  ICF catalog                                  _  Unix filesystem activity
_  VSAM catalog                                 _  IP connection activity
_  Basic report for unsupported records
```

Figure 469. EVENTS CUSTOM display panel

Use this panel to specify a custom display, a custom summary, or both. As an alternative, you can use any of the predefined detail layouts. In the preceding example, the predefined job and data set activity layouts have been selected. All record types not fitting these layouts are skipped. This processing behavior means that you can use the predefined layouts are therefore an additional selection mechanism.

The custom display panel is followed by the processing options menu. Depending on your query, you should make use of the CKFREEZE and completion options. In the example query, the **Complete with SAF data** option should be selected. (Without it, selection of data set activity records by RACF user ID would fail.)

After processing, the usual record overview and detailed display panels are shown. The panel in Figure 470 shows an overview panel with data set activity records.

```
Event log record detail information                    10 s elapsed, 4.5 s CPU
Command ===> ____________________________________________ Scroll===> CSR
                                            2Sep93 01:30 to  3Sep93 05:30
   Date      Time  Description
__ 02Sep1993 01:49 Output activity for non-VSAM data set R#BB.SMFMVS.G3623V00
s_ 02sep1993 01:53 Output activity for non-VSAM data set R#BB.SMFMVS.G3623V00
__ 02sep1993 09:10 Output activity for non-VSAM data set R#BB.SMFMVS.G3624V00
__ 02sep1993 14:54 Output activity for non-VSAM data set R#BB.SMFMVS.G3624V00
__ 02sep1993 16:28 Output activity for non-VSAM data set R#BB.SMFMVS.G3624V00
****************************** BOTTOM OF DATA ********************************
```

Figure 470. EVENTS CUSTOM overview display

Select any record for a detail display, in this case a data set activity record display.

```
Event log record detail information            Line 1 of 25
Command ===>                                                Scroll===> CSR
                                                 2Sep93 01:30 to  3Sep93 05:30
  Description
  Output activity for non-VSAM data set R#BB.SMFMVS.G3623V00

  Record identification
  Jobname + id:  R#BBMAN
  SMF date/time: Thu  2 Sep 1993 01:49:37.12
  SMF system:    IPO1       record type:  15     record no:  SMF10 9

  MVS event data
_ Dsname:   R#BB.SMFMVS.G3623V00
  Volser:   SYSMF3
  Unittype: 3480
  Catalog:

  RACF event data
  Access used:  UPDATE
  Class:    DATASET
  Profile:  R#BB.*.*.**
  Resource: R#BB.SMFMVS.G3623V00
  Level:     0

  RACF identification data
_ Userid:   R#BBMAN    Group: SYSOPR     Terminal:
  Name:
  Instdata:
****************************** BOTTOM OF DATA ******************************
```

Figure 471. EVENTS CUSTOM detail display

Batch SMF processing

This manual gives most attention to the Security zSecure ISPF interface. However, Security zSecure can also be used in batch mode. This section describes how to use the batch mode.

Table 265. Batch SMF processing commands and functions

Command or Function	Description
Run in background	Use the Output/Run option available on the Event panels to generate the Event query and submit a batch job to generate the report types selected
CO Commands	Use this Security zSecure main menu option to submit custom queries or queries from CARLa libraries. The SCKRCARL data set provides sample batch reports that can be used as is, or customized based on your reporting requirements.
Custom JCL	To create your own JCL to submit the Security zSecure batch job, start with the JCL samples in the SCKRCARL data set, or the JCL generated by Security zSecure when you submit a background job.
Create custom reports	In your own JCL, you can use the INCLUDE command to imbed CARLa scripts from the SCKRCARL data set or your own libraries. You can also use the full Security zSecure language (CARLa) to create your own custom reports. When you create your own queries, read the SMF language reference at least once. See "SMF reporting using predefined CARLa scripts" on page 590 for an overview of the sample reports included with Security zSecure. We advise you to read, then try the SMF batch reports CKALF... at least once.

Tip: When submitting a batch job from the Security zSecure ISPF application, you can specify tape data sets using option **5** SELECT on the SUBMIT panel. This allows you to read SMF data sets from tape without MOUNT authority.

SMF reporting using predefined CARLa scripts

Security zSecure provides sample reports in the SCKRCARL library. These reports are created from scripts written in the CARLa programming language. The convention used to name CARLa scripts is explained in "Naming convention" on page 706.

You can run these sample scripts directly or access the functionality from the IBM Security zSecure user interface. You can also modify the existing scripts to develop your own custom reports using the standard display formats provided in the sample files.

For details on these scripts, see the following sections.

- "Field definitions for SMF and other log files"
- "Using record display scripts for interactive reporting" on page 591
- "Batch reports" on page 592

Field definitions for SMF and other log files

The CARLa Auditing and Reporting Language (CARLa) allows you to define variables for parts of SMF records, and then use them in reporting. You can also define the layouts of other logs using the DEFTYPE command. Table 266 lists the CARLa scripts that include such definitions (CKAS*), Many of these scripts are used for the reports in the following sections.

Table 266. CARLa scripts that define variables for fields in SMF records

Member	Definitions
CKASKERB	Kerberos fields (in RACF relocate sections 331 through 335)
CKASSECP	SecurPass fields
CKASUSS	z/OS Unix System Services fields (in RACF records)
CKASWBAC	HTTP access log (DEFTYPE TYPE=WEBACCESS)
CKASWBER	HTTP error log (DEFTYPE TYPE=WEBERROR)
CKAS0119	SMF record type 119 subtypes 48-52 (CSSMTP client)
CKAS0033	SMF record type 33 (APPC Transaction Record)
CKAS0080	SMF record type 80/83 (RACF and R_auditx records)
CKAS0081	SMF record type 81 (RACF initialization)
CKAS0089	SMF record type 89 (Usage data)
CKAS0090	SMF record type 90 (System status)
CKAS0092	SMF record type 92 (z/OS UNIX System Services)
CKAS0102	SMF record type 102 (DB/2)

Using record display scripts for interactive reporting

The SMF record display scripts which start with the name pattern C%ADF are used by the interactive component of Security zSecure to generate SMF data reports for the ISPF display. Many of these scripts cannot be run directly as a library member.

These CARLa scripts typically define a display for a specific group of SMF records such as ICF catalog records. If you follow the conventions used by Security zSecure, you can include these display layouts in your own queries.

To follow the convention for creating an SMF report, use the following process:

- Create a SMF NEWLIST with the name SMFSEL and output limit 0.
- Use SELECT and EXCLUDE statements to select the records you are interested in.
- Include a fake LIST, SORTLIST, or DISPLAY command.
- Then include any SMF sample member. The CARLa scripts select the records fitting their layout from the selection of the NEWLIST named SMFSEL, and using the appropriate DISPLAY commands to show all relevant data from those records types.

The following sample query shows the Security zSecure convention for coding report data. The query selects records from users `JOHN`, `DAVE`, and `PETER`, and then includes the CARLa scripts defining data set and `ICF` catalog activity.

```
newlist type=smf name=smfsel outlim=0      /* Required newlist */
select user=(john dave peter)              /* Selection */
list type                                  /* Fake list command */
i m=ckadfdda                               /* Data set activity */
i m=ckadfdic                               /* ICF Catalog */
```

Table 267 describes the SMF record display scripts. You can access these record display from the menu structure.

Table 267. IBM Security zSecure SMF record display scripts

Member	SMF record types
CKADFDAR	RACINIT record layout from SMF type 30
CKADFDDA	Data set activity
CKADFDFS	z/OS UNIX file activity
CKADFDIC	ICF catalog activity
CKADFDJA	Job activity
CKADFDOT	Miscellaneous 'other' records
CKADFDRA	RACF processing records (defines various display layouts, depending on event type)
CKADFDRS	RACF processing records (one display layout, can be used with a SUMMARY)
CKADFDVS	VSAM catalog activity
CKADFDZZ	Common SMF header display
CKADFD02	DB/2 record types 100, 101, and 102
CKADFD81	RACF status record display in format like CKRDSR80
CKADFD90	MVS event information: defines displays for IPL reason and down time, SRM data, LOGREC, SMF stop and switch events

Table 267. IBM Security zSecure SMF record display scripts (continued)

Member	SMF record types
CKADFJOB	Summary of activity by user and job
CKADFJ33	APPC transaction summaries
CKADFSUM	Summary of record types selected
CKADFTCP	TCPIP activity
CKADF109	Firewall activity

Batch reports

Table 268 describes the reports you can run using a batch process.

Table 268. zSecure Batch reports

Report	Meaning
CKALFDES	Overview of record descriptions
CKALFDEV	Find use of a specific device type
CKALFJES	Show JES2 related logging
CKALFJOB	Overview of job activity for selected users (must be edited before it is used)
CKALFJVI	Jobs with failures
CKALFJ33	APPC transaction overviews (partner LU and local LU overviews, local user ID and group overviews)
CKALFNPR	Find access to data sets without RACF profile. Can be used to find potential PROTECTALL problems
CKALFREV	Generate a REVOKE for users with too many password or password phrase changes (review before using)
CKALFRST	RACF daily statistics of logon and access events, and the number of violations
CKALFRVR	Revoke and resume summaries by user and by administrator
CKALFR80	RACF daily report of violations, special/operations activity, audited users, RACF command use, command violations, and all non-success records
CKALFR81	RACF IPL status records, format compatible with CARLa script CKRLSR13
CKALFSEL	(Dummy) selection NEWLIST SMFSEL
CKALFSTA	RACF event counts by hour
CKALFSTB	RACF event counts by time of day
CKALFSTC	RACF event counts by weekday
CKALFSUM	SMF record summary table
CKALFTAP	Find users of round tapes (can be edited to select other unit types)
CKALFUSR	User audit trail (the user ID must be configured before the CARLa scripts are run)
CKALFVW	RACF violations and warnings

Chapter 8. RACF Offline

The RACF Offline function available with zSecure Admin allows you to execute and test most RACF commands against an offline or inactive RACF database.

The following terms are used to distinguish between the inactive RACF database and the system RACF database.

- *Offline RACF database* and *Offline RACF environment* describe the inactive RACF database and its environment.
- *System RACF database* and *System RACF environment* describe the RACF database that is currently used by the system for all regular verifications.

For most installations, the System RACF database consists of a primary and secondary (backup) database. The Offline RACF database does not provide such an automatic backup feature.

In the standard RACF environment, all RACF verifications (like logon and access to data sets) are verified using the information in the primary RACF database. All updates are normally performed against both the primary and the secondary (backup) RACF database. Thus, if a RACF administrator issues a command to add a profile, the new profile is added to both databases.

Using RACF Offline you can direct all RACF *commands* to a third or alternate RACF database. RACF *access verifications* are not affected and are still performed against the System RACF database. Thus, the Offline RACF environment applies only to the RACF commands. RACF Offline must be explicitly activated before it is available. After the Offline RACF environment is stopped, the regular System RACF environment is re-established. Currently, you *cannot* use the Offline RACF environment for logon and resource access verification. These functions are always performed against the System RACF environment.

As an illustration of the difference between the handling of *commands* and *verifications*, consider the situation when a user issues the ISPF command while in the Offline RACF environment. All standard ISPF functions remain available. Depending on the type of actions being performed while in ISPF, either the System RACF database or the Offline RACF database is used. For example, when the user uses Option-1 to BROWSE a data set, the System RACF database is used to verify READ access to the data set. If the user uses Option-6 or the RACF panels to issue a RACF command, the Offline RACF database is used. The main thing to remember is that only the RACF commands are affected by RACF Offline.

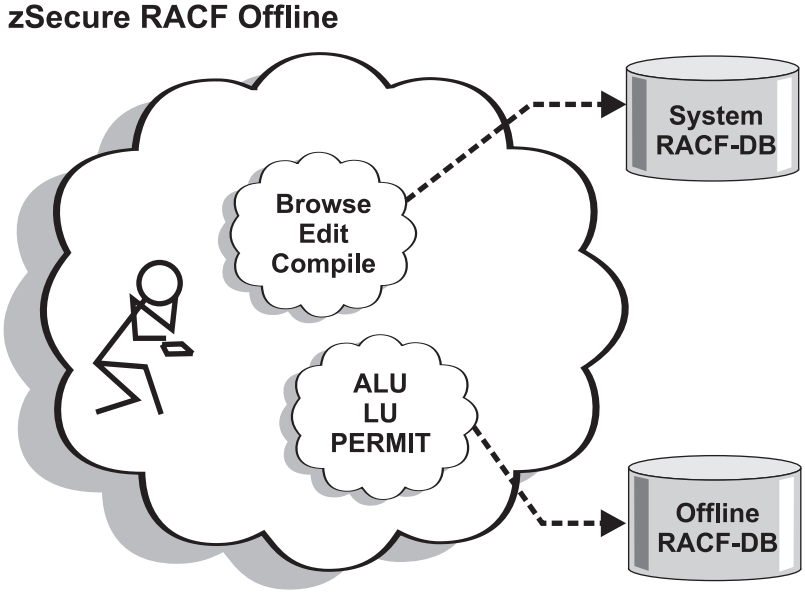


Figure 472. RACF commands and access verification in Offline RACF environment

The environment, as set up using the B8RACF command, can be compared with an RRSF environment. Whenever you are in the Offline RACF environment, it is like automatically adding the AT keyword to each and every RACF command. It looks like the command is always sent to another system, which uses another RACF database.

The Offline RACF environment supports most RACF commands and supports some non-RACF commands. The following RACF commands are not supported in the Offline RACF environment.

- Operator RACF commands
- RACLINK command
- RVARY command
- SETROPTS command

The ISPF command is an example of a non-RACF command that is supported in the Offline RACF environment. You can still run most non-RACF commands inside the Offline RACF environment by first running the ISPF command and then using the ISPF option 6 to issue all other commands.

You can start the environment interactively under TSO, but you can also run the B8RACF command in a batch job. All functions are available both in TSO and in batch. For additional information, see “The environment” on page 596.

To begin using the Offline RACF environment, issue the B8RACF command. Next, when prompted, run the LOGON command. In the Offline RACF environment, the LOGON command builds a security environment based on the authorizations in the Offline RACF database. If you do not use the LOGON command, the USERID of the terminal user must also be present in the Offline RACF database, or the USERID must have system-SPECIAL authority. See “Logging on to the Offline RACF database” on page 600.

Functions and usage

After starting RACF Offline, a user experiences two different environments. The regular System RACF environment that is used for logon and access verification, and the Offline RACF environment that is used for all RACF commands. As soon as the user exits B8RACF, the RACF commands use the System RACF database again. The B8RACF command facilitates switching between different RACF databases.

To avoid confusion, use the Offline RACF environment for dedicated sessions. If you are in the Offline RACF environment, the output from the LD command shows a different RACF profile than the one that is used for data set access verification which might be confusing. Or, for example, the LD command can show `your access=alter` at the same time that you get access violation messages showing the same profile. Before using B8RACF on a daily basis, try it and learn about the confusing aspects of the mixed environment within ISPF.

Figure 473 illustrates the use of B8RACF to establish an Offline RACF environment.

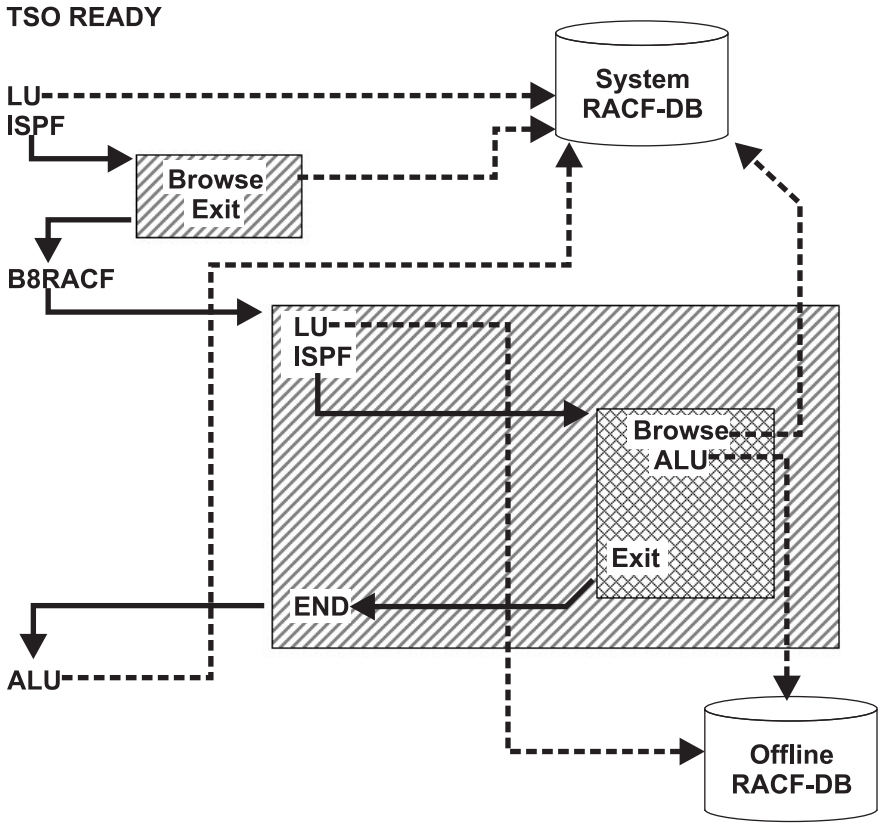


Figure 473. RACF commands and access verification in Offline RACF environment

In Figure 473, several commands are issued, and the flow of commands follows the solid arrows. The dotted arrows show use of a particular RACF database. The backslashes (\\\) box indicates the ISPF environment, and the forward slash (///) box indicates the B8RACF environment. The crosshatched (XXXX) box indicates use of ISPF inside B8RACF. Access verification follows these processing steps:

1. The first LU command is issued in TSO READY mode (line mode) and accesses the System RACF database (dotted arrow).

2. Inside the first ISPF session, the System RACF database is used as well. After issuing the B8RACF command, the LU command accesses the Offline RACF database.
3. As shown inside the crosshatched (XXXX) box in Figure 473 on page 595, the BROWSE function of ISPF still involves the System RACF database, and the ALU uses the Offline RACF database.

In summary, access verifications always use the System RACF database. RACF commands go to the System RACF database when operating outside of B8RACF and to the Offline RACF database when inside B8RACF.

The environment

The environment that is set up using the B8RACF command can be compared in some respects to an RRSF environment. Whenever you are in B8RACF, it is like automatically adding the AT keyword to each and every RACF command. It looks like the command is always sent to another system, which uses another RACF database.

In the Offline RACF environment:

- Access checking is done against the System RACF database.
- Commands are directed to the Offline RACF database.
- Commands are parsed according to the settings of the active system.

  This includes both the SETROPTS settings (GENERIC, GENCMD and EGN) and the dynamic parsing (as set by the IRRDPI00 command). A fully initialized version of RACF on the active system is required.
- The Custom Data fields (in USER and GROUP CSDATA segments) as defined in the CFIELD profiles are used from the active System RACF database. These definitions are installed into common system storage using the IRRDPI00 command. RACF Offline does not provide an option to use IRRDPI00 to activate the Custom Data definitions from the Offline RACF database. Therefore, inside RACF Offline, parsing and handling of Custom Data fields is done using the definitions as installed from the System RACF database.
- Field level access checking uses the profiles as defined in the Offline RACF database. Previous versions of the RACF Offline program used the in-storage authorizations from the System RACF database. This behavior was changed in IBM Security zSecure Admin release 1 version 10.
- Other RACF command authorizations are done using information from the Offline RACF database.
- Profile actions that are not commands are directed to the System RACF database. For example, in the Offline RACF environment when you delete a data set that is protected by a discrete profile, that profile is deleted from the System database.
- In releases of the RACF Offline program before version 1.9.1, updates made via the IBM Security zSecure Admin CKGRACF function were directed to the System RACF database. Starting with version 1.10, these type of updates are directed to the Offline RACF database. Authorization for the CKGRACF function is obtained from the Offline RACF database.

Activating

The RACF Offline functions are not available until the program is explicitly activated by using the B8RACF command. The B8RACF command can be executed interactively under TSO, but you can also run the command in a batch job. If you submit a batch job, the job is executed in the standard System RACF environment.

The batch job also needs to explicitly switch to an Offline RACF environment. Switching environments in a batch job can be done by using either of the following methods.

Method 1

Issue the B8RACF command as a regular command under the TSO batch environment.

If you use this method, you should use one of the alternative TSO programs IKJEFT1A or IKJEFT1B instead of the default IKJEFT01 program.

When using IKJEFT1A, the entire job is terminated if an error occurs that prevents the B8RACF command from executing. This results in flushing all B8RACF RACF commands. If the default TSO program IKJEFT01 is used, TSO execution would continue, and all RACF commands would be executed against the System RACF database. To prevent this from happening, one of the alternative programs should be used. The following example executes the B8RACF command as a TSO batch job.

```
//RUNIT    EXEC PGM=IKJEFT1A
//STEPLIB  DD DISP=SHR,DSN=BYBG.ROFFLINE.SB8RLOAD
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 B8RACF
 ALU BCSCTST REVOKE
 END
```

Method 2

Issue the B8RACF command in a job step program.

The B8RACF command should be specified in the `PGM =` keyword on the EXEC statement of the job step. The B8RACF program uses the same *input* and *output* `ddnames` as used under TSO (respectively SYSTSIN and SYSTSPRT). If an error occurs in the B8RACF command, the remaining commands in the SYSTSIN stream are automatically discarded. The following example executes the B8RACF command as a JCL job step.

```
//RUNIT    EXEC PGM=B8RACF
//STEPLIB  DD DISP=SHR,DSN=BYBG.ROFFLINE.SB8RLOAD
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 ALU BCSCTST REVOKE
```

The Offline RACF environment that is started from a TSO user or a batch job is never automatically propagated to other jobs. At first, when you are frequently using batch jobs to execute RACF commands, you might be confused. RACF commands are only directed to the Offline RACF database after you have explicitly activated the environment.

Supported file definitions for the B8RACF command

The following DD statements (or file allocations) are used by RACF Offline.

STEPLIB

STEPLIB or JOBLIB identifies the library containing the RACF Offline program modules.

SYSTSPRT

Defines a sequential message output data set. SYSTSPRT can refer to a sequential data set, a member of a partitioned data set, or a SYSOUT data set. The data set can have variable or fixed length records. Use of a sufficiently large logical record length (for example 255 bytes) ensures that output records are not folded across multiple output lines.

SYSTSIN
Defines a sequential command input data set. This file must contain RACF or RACF Offline supporting commands as described in section "The B8RACF command and Control commands" on page 612.

SYSTSIN can refer to a sequential data set, a member of a partitioned data set, or SYSIN data set. The data set can have variable or fixed length records. Use of 80-byte fixed length records is convenient for most situations. Continuation lines are supported using the TSO convention of a + (plus) or - (minus) as last non-blank character in the available input line. The following processing rules are used for SYSTSIN fixed and variable length data sets:

Fixed length data set (FB) – The last 8 bytes of the record are treated as a sequence number and ignored.

Fixed length data set with ASA control characters (FBA) – The first byte of the record is treated as a carriage control character and ignored.

Variable length data set (VB) – The first 8 bytes of the record are treated as a sequence number and ignored.

Variable length data set with ASA control characters (VBA) – The first 9 bytes of the record are treated as a sequence number, followed by a carriage control character and ignored.

SYSPRINT
Defines an internal work file. The ddname is freed and reallocated by the B8RACF program.

INDD*n*
Defines the RACF input data set that makes up the RACF database. These ddnames are used for the RACF database as specified in the RACFDB command. If no RACFDB command is issued, the program assumes that INDD*n* defines the Offline RACF database to be used.

OUTDD
Defines an internal work file. The ddname is freed and reallocated by the B8RACF program.

B8RPARM
Defines a sequential parameter input data set. This file must contain RACF Offline control commands as described in section "The B8RACF command and Control commands" on page 612. B8RPARM can refer to a sequential data set, a member of a partitioned data set, or SYSIN data set. The data set can have variable or fixed length records. Use of 80-byte fixed length records is convenient for most situations. The line continuation, sequence number, and ASA control characters for SYSTSIN also apply to B8RPARM.

B8ROPTnn
Defines a sequential parameter input data set. This file must contain RACF Offline control commands as described in section "The B8RACF command and Control commands" on page 612. B8RPARM can refer to a sequential data set or a member of a partitioned data set. The data set must have fixed length records of 80 characters. Continuation lines are not supported and all 80 characters are interpreted as part of the command.

Using RACF and non-RACF commands

As mentioned in the previous section, the Offline RACF environment only supports a limited set of commands. However, because ISPF is one of the supported commands, you can execute all other commands from inside ISPF. The

following non-RACF commands are also directly supported in B8RACF: LOGON, END (or EXIT), and several internal commands (logging control and switching of the Offline RACF database).

The END command signals termination of B8RACF. See “Supporting commands” on page 615 for more information on these commands.

The following RACF commands are *not* supported in the Offline RACF environment:

RVARY
The RACF RVARY command is used to switch or (in)activate RACF databases for the entire system. The equivalent function in is provided using the B8RVARY command. (See “**B8RVARY**” on page 617.

SETROPTS
The SETROPTS command is not supported because it is not currently feasible to translate its functionality to the Offline RACF environment. In addition, the potential impact of accidentally issuing the SETROPTS command in the wrong environment is an unacceptable risk.

RACLINK
Because the RACLINK command is mainly executed in the RACF address space, it is currently not enabled in the Offline RACF environment. Issuing the command results in a request to the RACF address space which would subsequently update the System RACF database instead of the Offline RACF database. Because this is not the desired effect, the RACLINK command is not supported.

Preparing a RACF database for RACF Offline use

You can use any RACF database as an RACF Offline database except the active System RACF database. In addition, do not use a RACF database that is currently in use by a different z/OS system or by a z/VM system. Through shared DASD, you can use a foreign database, but for serialization reasons it is not a good idea to use one. However, you can use a foreign database for recovery when no other system that can use it is active. Also, be aware that most foreign systems have a primary/backup database combination. If you are working with a system that uses a primary/backup database combination and update only one of the databases, the primary and backup databases will be out of sync. To resynchronize the databases, you copy the updated database over the other one before you IPL any system that uses the databases.

During RACF Offline initialization, the RACF Offline code checks that the database is not incorrectly shared with any other system. This is implemented via `IRRPLEX_<sysplex-name>` profiles in the GXFACILIT class as described in "Guarding against data corruption resulting from incorrect database" in the *Security Server RACF System Programmer's Guide*. If the Offline RACF database contains profiles indicating the RACF database has been used in data sharing mode, RACF Offline issues a warning message and a prompt to continue. If you are sure that the RACF Offline database is no longer part of an active data sharing group, you can respond with *continue*. In that case, RACF Offline verifies that you have at least CONTROL access to the resource `B8R.RACFDB.offline-database-name`. If RACF Offline does not detect any profiles indicating use of the Offline RACF database as part of a data sharing group, processing continues without any prompts to the user. To record that the Offline RACF database is now used by RACF Offline, an `IRRPLEX_<sysplex-name>` profile is added indicating non-data sharing mode. If RACF Offline ends processing normally, with no abends, the `IRRPLEX_<sysplex-name>` profile is removed again. The `sysplex-name` used by RACF Offline is `B8RACF`

followed by two numeric characters representing the RACF Offline session. An example of such a sysplex-name is B8RACF01.

After creating a fresh copy of the RACF database, you might need to respond to the B8R351A prompt to continue. To avoid being prompted each time that you use this database, use a USERID with system-SPECIAL to remove the IRRPLEX_* profiles in the GXFACILI resource class.

If the Offline RACF database is activated as a System RACF database on another system (either via IPL or RVARY), the other system might detect that RACF Offline is using the Offline RACF database in a non-data sharing mode (indicated via sysplex name B8RACFnn). If this situation is detected, the other system issues one or more prompts to the console operator. Of course, these console messages are only issued if the Offline RACF database is still in use, or if RACF Offline failed to remove its IRRPLEX_sysplex-name profile. These console messages are only available for z/OS Release 1.10 or later.

Note: An inappropriate continue response to the console messages will most likely result in corruption of the Offline RACF database.

When using an existing database, make sure that the templates in that database are on a level that is supported by the level of RACF on the active system. Using downlevel templates might result in error messages such as IRR51004I, IRR51011I, or IRR52115I, or in ABEND 483-024. If these errors occur, upgrade the templates by running IRRMIN00 with PARM=UPDATE against the Offline RACF database. Use the IRRMIN00 utility and the templates from the system where you are using IBM Security zSecure Admin RACF Offline.

If you are not using a foreign database, copy an active System RACF database or initialize a new database for use as an Offline RACF database. Normally, you use IRRUT200 to copy the active System database. If the active System database is physically split into multiple databases, you might need to use IRRUT400 for the copy process. RACF Offline requires that the Offline RACF database is physically split in the same way as the active System RACF database. If the source database uses a different physical split other than that used on the system where you want to execute, copy the database using IRRUT400 and create the output data sets such that the data sets match the physical split used on the execution system.

Logging on to the Offline RACF database

To run the B8RACF command, the user must be logged on the system. If the terminal user does not explicitly log on inside the Offline RACF environment, the authorization of the user in the System RACF database is used for the Offline RACF database. This authorization can cause several problems if the terminal user is not defined in the Offline RACF database. The most common symptom of such problems is the error message:

```
ICH51011I RACF MANAGER PROCESSING ENDED DUE TO ERROR. RETURN CODE = 24
```

This error message indicates that RACF was unable to obtain the authority of the current user to execute the requested command. Other possible error messages include:

```
ICH51003I NAME NOT FOUND IN RACF DATA SET
```

which often indicates that a userid or group that is used as the default in a RACF command (for example, the default group for the current user) does not exist in the Offline RACF database.

If the terminal user has the system-SPECIAL attribute, most of the preceding problems are not immediately obvious. However, the system-SPECIAL attribute must be assigned in the System RACF database to be effective, which is impractical in most situations.

The real solution to these problems is to start issuing the RACF Offline commands with a LOGON command to build an authorization environment by using the information from the Offline RACF database. The simplest form of the command is `LOGON` without any additional parameters. When this command is issued, the current `userid` is used to log on to the Offline RACF database. If the current userid has insufficient authority or is not defined, use the extended form of the command, `LOGON` *`userid`*`/` for example. This extended command prompts for the password and logon to the Offline RACF database using the specified userid. If you are properly authorized in the System RACF database, you are able to use the LOGON command with the SPECIAL keyword. If you use the SPECIAL keyword, your session uses the RACF system-SPECIAL attribute while using the Offline RACF database. The system-SPECIAL attribute is temporary and is used only if the SPECIAL keyword is used with the LOGON command. See "Supporting commands" on page 615 for the complete syntax of the LOGON command.

Switching between RACF databases

You can use the B8RVARY command to switch to another Offline RACF database without leaving the B8RACF command environment. The B8RVARY command can be used directly inside B8RACF, but the command is also available under ISPF. The B8RVARY command can be used interactively or through existing option files.

Switch RACF databases using the B8RVARY command interactively

Use this interactive procedure to switch to RACF databases without leaving the B8RVARY command environment.

1. Run the B8RVARY command.
2. When prompted, confirm that you want to change the Offline RACF database.
3. If you respond with `YES`, the current Offline RACF database is closed and freed.
4. When prompted, enter the B8RACF Control commands.

   The most likely commands to use are the RACFDB command and the LOGDS command.
5. When the specification of the Offline RACF environment is complete, use the END command to stop the prompts.

Switch RACF databases using an option file

Instead of using the B8RVARY command interactively, you can also use a prepared option file. The option file contains the required B8RACF control commands to switch to another RACF database.

The preallocated configuration files are easier to use, especially when you need to switch frequently between different Offline RACF databases. The preallocated configuration files are also used for the REPLAY function. See "Replaying previously issued commands" on page 603.

The option file is a data set that contains B8RACF Control commands as shown in the following example:

```
/* Options file for old z/OS 1.5 database */
racfdb 'sys1.racf15'
logds 'sys1.racf15.b8rlog'
smf id($150)
```

To use this predefined environment, allocate the data set to the ddname B8ROPT*xx*, where *xx* is any two alphanumeric or national characters as shown in the following example.

```
alloc da('BYBG.B8ROPT.CNTL(RACF15)') fi(B8ROPT15) shr
```

In this example we assume that the data set containing the B8RACF Control commands is the member RACF15 in partitioned data set BYBG.B8ROPT.CNTL. The B8ROPT*xx* file to be used is B8ROPT15. After allocating the file, it can be used in the B8RVARY command with the SELECT keyword.

```
  Menu  List  Mode  Functions  Utilities  Help
------------------------------------------------------------------------
                               ISPF Command Shell
Enter TSO or Workstation commands below:

===> b8rvary select(15)_____________________________________
_______________________________________________________________________
_______________________________________________________________________

Place cursor on choice and press enter to Retrieve command

=>
=>
=>

B8R228I Start processing B8ROPT15
B8R274I RACF DB to be used is SYS1.RACF15
B8R268I LOG data set to be used is SYS1.RACF15.B8RLOG
B8R304I New SMF-ID: $150
B8R238I Completed processing B8ROPT15
***
```

Figure 474. Using the B8RVARY command with the SELECT keyword

Logging for RACF Offline commands

You can maintain a log of all RACF commands issued during a B8RACF command session. To enable this function, you need a predefined log data set that can be designated as the log file. Then, use the LOGDS control command to specify the log file.

When setting up the data set to be used for logging, the following requirements and processing considerations apply:

- Define the log data set before using the LOGDS command to specify the log file.
- Specify the data set as VB (variable blocked) with LRECL 255 (record length of 255 bytes).
- Optional: Specify a block size of 27998 for the block size which is the system determined optimum block size for 3390 disks).

The following process considerations apply to the LOG file.

- The LOG data set is used in extend mode, which means that all logged commands are added to the end of the LOG data set.
- Using default data set characteristics, the LOG data set can contain on average 10000 commands per cylinder on disk.

- As a best practice, use one LOG data set for each Offline RACF database so that the LOG contains all changes relevant to a particular database. You can add the data sets easily by adding a LOGDS command in either the B8ROPT module, the B8RPARM file, or the B8ROPTxx control files.
- If the LOG data set is full, logging is suspended. To keep the log from getting full, either allocate a sufficiently large LOG data set, or RESET the LOG file periodically.

Replaying previously issued commands

The LOG data sets can also be used as command source for the B8REPLAY command. The B8REPLAY command specifies a preallocated B8ROPT*xx* control file.

```
B8REPLAY SELECT(xx)
```

The B8ROPT*xx* control file is scanned for a LOGDS command. The LOGDS command designates the source for the commands that should be executed against the current Offline RACF database. The following example shows a B8ROPT*xx* control file.

```
/* Sample RACF Offline Options file */
RACFDB 'BYBG.ROFFLINE.TESTDB'
LOGDS  'BYBG.ROFFLINE.TESTDB.LOG'
SMF ID($B8R)
```

To avoid problems, command logging is temporarily suspended during replay of commands.

You can also use the B8REPLAY command to execute previously prepared RACF commands by creating a B8ROPTxx file containing only the LOGDS statement. The LOGDS statement should point to an existing data set containing the commands you want to issue. The data set should have the attributes VB(255). Data sets with a fixed record length are currently not supported. The records should not contain line numbers, and cannot have any continuation records.

Auditing

Most of the standard RACF command processors write SMF records during processing. It is almost impossible to distinguish the SMF records written for an update to the Offline RACF database from those written for an update to the active System RACF database. To enable identification, you can use the SMF command to mark SMF records as written during a session. Some of these options apply to all SMF records. Others only apply to the RACF SMF records. The best option is to modify the SMF ID for the affected records.

The modification of the SMF records is performed by the dynamic activation of the SMF record exit routines (IEFU83, IEFU84, IEFU85). However, this is dependent on the installation SMF options. For this reason, you should always specify EXITS(IEFU83,IEFU84,IEFU85) in the active SMFPRM*xx* member of PARMLIB for all subsystems (or for the entire system). These exits should be specified, even if the installation itself does not provide any exit routines. In the absence of any installation provided SMF exits, the IBM-provided dummy modules in LPALIB are used.

Because RACF Offline uses the dynamic exit facility, the installation should also use dynamic SMF exits (defined by PROG*xx* in PARMLIB) instead of static routines linked into LPALIB. Of course, this only applies if the installation requires SMF exits for exit points IEFU83, IEFU84 or IEFU85.

Using RACF Offline

This section provides some guidelines for selecting the various control command options, depending on the intended functionality. "RACF Offline commands" on page 611 describes the various control commands. For information about how some of these can be issued automatically at every invocation of the B8RACF command, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

When you start using the B8RACF command, B8RACF processes control commands from two input sources. One input source is created during installation, the other is variable, and can be selected by the user. During installation, the B8ROPT module is assembled and included in the B8RACF module. It is always executed before other processing takes place. We recommend that the module contain an SMF command to indicate default processing of SMF records created during usage. The SMF command has several options to uniquely identify such SMF records. If no SMF command is used, the RACF SMF records created during use of RACF Offline cannot be distinguished from those created by RACF commands outside RACF Offline. Because this is undesirable, we recommend that the SMF Control Command is used in B8ROPT. Use of the SMF command in B8ROPT is not RACF controlled. This means that the user does not need any RACF authorization for the SMF option specified by B8ROPT to become effective. Optionally, the B8ROPT module can contain a RACFDB command, and a LOGDS command to specify defaults for the RACF database and log file. If the user does not have sufficient authority to use the selected database as the Offline RACF database, the command fails.

At the discretion of the user, it is also possible to include control commands in the B8RPARM file. When this file is allocated, its contents are used to override the options specified by B8ROPT. One of the differences between the use of B8ROPT and B8RPARM is that the commands used in B8ROPT are not subject to the command-authorization-verification process, while those in B8RPARM are.

Allocating the `B8RPARM` file to the terminal provides the greatest flexibility. This allocation allows the user to dynamically select which RACF database and which SMF options to use.

For both uses of the `B8RPARM` file, the terminal user must be authorized for the options specified. If the terminal user lacks sufficient authorization, the options specified in `B8ROPT` cannot be overruled, and the defaults are enforced. This is the main reason that use of the SMF command in `B8ROPT` is strongly advised. It provides a way to ensure that only selected users are permitted to modify the SMF processing options.

In respect to the preceding considerations, the following different uses are anticipated.

Controlled usage
The B8ROPT module specifies the SMF options, and also includes a RACFDB command to specify the RACF database to be used. By default, the B8RPARM file is *not* allocated. The users do not have any authorization to specify any SMF processing options, and thus the installation specified options are used. The intended terminal users are explicitly authorized to use the selected RACF database. Users who are not permitted to access functions could be excluded from access to either the `B8R.RACF.OFFLINE` profile, or from access to any `B8R.RACFDB.`*dsname* profile. Without access to *any* Offline RACF database, RACF Offline cannot be used.

If the user allocates the B8RPARM file, she would still not be able to select databases other than the ones explicitly permitted by B8R.RACFDB.dsname profiles. Lacking sufficient authorization, the SMF options could not be modified either.

The suggested access to the control profiles for this type of user would be:

```
B8R.RACF.OFFLINE                                READ
B8R.RACFDB.the-database-specified-in-B8ROPT     UPDATE
B8R.SMF.**                                      NONE
```

User-specific default use

The B8ROPT module specifies the SMF options, and also includes a RACFDB command to specify the default RACF database to be used. Users would normally allocate the B8RPARM file to an input data set containing the appropriate RACFDB command to select the database intended for their use. The RACFDB commands should point to an existing RACF database. The terminal user needs access to the B8R.RACFDB.*dsname* profile controlling usage of the RACF database specified by their B8RPARM file.

If the user changed the allocation of the B8RPARM file, she would still need sufficient access to the selected RACF database.

The suggested access to the control profiles for this type of user would be:

```
B8R.RACF.OFFLINE                                READ
B8R.RACFDB.the-database-specified-in-B8ROPT     UPDATE
B8R.RACFDB.other-approved-database              UPDATE
B8R.SMF.**                                      NONE
```

Flexible usage

The B8ROPT module specifies default options for both the SMF options and the RACF database to be used. The B8RPARM file is allocated to the terminal. During startup of B8RACF, the user enters additional control commands to specify SMF processing options, and to specify the RACF database to be used. Because the SMF command does not have an option that resets the processing to do nothing, the SMF records are always processed in some way. (Processing includes suppression of those records.) The terminal user must be authorized to use the RACF database selected for usage.

The suggested access to the control profiles for this type of user would be:

```
B8R.RACF.OFFLINE                                READ
B8R.RACFDB.the-database-specified-in-B8ROPT     UPDATE
B8R.RACFDB.**                                   UPDATE
B8R.SMF.**                                      UPDATE
```

In summary, by selecting the appropriate defaults in B8ROPT, in combination with prepared B8RPARM files and appropriate RACF profiles, the installation accommodates different types of users. It is anticipated that most installations will use all three methods, depending on the need of their users.

Usage scenarios

Several applications for exist. This section describes some of the more common situations.

Preparing large updates

This section discusses two large update processes, RACF database merge and an ACF2 to RACF conversion which would typically require significant system downtime. The example shows how can be used to accomplish the same tasks while minimizing downtime.

RACF database merge: Merging RACF databases can be done using the MERGE function of IBM Security zSecure Admin. The output of the MERGE function is a stream of RACF commands that needs to be executed. Usually, the commands are executed on the target system to modify it in such a way that the profiles from the source system are added. The resulting database is then used during a test period. If the test fails, you probably discard the RACF database, and try again. The alternative to discarding is a one-time merge, followed by incremental corrections. You are now faced with a dilemma: If you discard the RACF database, you need significant time on a dedicated system to rebuild it (possibly several times). If you use the one-time merge approach, you need significant testing beforehand to ensure that the resulting RACF database is acceptable for production usage. Either way, a dedicated system is needed during a significant period.

Alternatively, RACF Offline can be used on the existing target system. A copy of its RACF database is used as an Offline RACF database, and the stream of RACF commands from the MERGE function is executed. In the discard and iterate approach the following steps are used:

1. To start the test-period, the Offline RACF database is activated using either an IPL, or using a sequence of RVARY and RENAME commands.
2. At the end of the test, the inverse steps are executed to reactivate the previous System RACF database.
3. After the test, the input to the merge tool is tuned, and a fresh copy of the target RACF database is used for the next iteration.

In the *incremental correction* approach, the following steps are used:

1. After executing the stream of RACF commands from the merge tool on the Offline RACF database, you can use various reporting tools to inspect the resulting RACF database.
   - and regular RACF list commands
   - displays and reports
2. Using the reports about the Offline RACF database, you make manual adjustments to the profiles.
3. When the fine-tuning of the profiles is completed, the Offline RACF database is activated as the RACF System database.
4. If the user passwords need to be updated, you can run a final MERGE of all users, and select the CKGRACF commands that set the password and last-use dates.

ACF2 to RACF conversion: Another process that can require a lot of system downtime is conversion from a different security product such as ACF2. The output of the conversion process is again a stream of RACF commands that needs to be executed. Usually the entire conversion project involves building and testing the RACF system several times. Without RACF Offline, these commands must be executed on the System RACF database. Because the purpose of these commands is to define the group, user and resource profiles, the system cannot be used by regular users during this period. That means that the time available for testing is shortened significantly. One possibility to avoid this situation is to create a separate LPAR just for the execution of this stream of RACF commands. After building the new RACF database, the database is then moved to the test LPAR, and activated (either using IPL, or using a sequence of RVARY and RENAME commands).

When RACF Offline is available, an alternative exists. Instead of creating a separate LPAR, RACF Offline is used on the existing test LPAR. Now the commands are executed against an Offline RACF database. This can be done at the same time that the test LPAR is used for other work. After building the refreshed RACF database,

it can be activated as the System RACF database using IPL, or a sequence of RVARY and RENAME commands. The activation process should also involve creation of a backup RACF database.

Testing new profiles

In a customer environment a project was started to reduce the number of data set profiles. They used the *Report Redundant* function to compare each profile to its next-best generic. For example, when the profiles shown in Figure 475 are present, Profile 2 and Profile 1 are compared and the entry `XYZZY` on the access list is flagged as major difference. The entry `XYZZY` makes Profile 2 *non-redundant*. It is that entry that makes the profile different from the next best profile. This difference is what makes the profile *contribute* something to the security definitions. The installation (often the security administrator) has the option to decide that this contribution is *really* significant, or just a fluke that can be discarded.
Other observations about the list of profiles shown in Figure 475 are as follows:

```
1)   ABCD.**          UACC(NONE)      READ(XYZ,QWAS)                  AUDIT(FAIL(READ))
2)   ABCD.A*.**       UACC(NONE)      READ(XYZ,QWAS)  UPDATE(XYZZY)   AUDIT(FAIL(READ))
3)   ABCD.PROD.**     UACC(NONE)      READ(XYZ)                       AUDIT(FAIL(UPDATE))
4)   ABCD.TEST1.**    UACC(NONE)      READ(XYZ)       UPDATE(XYZZY)   AUDIT(FAIL(READ))
5)   ABCD.TEST2.**    UACC(NONE)      READ(XYZ)       UPDATE(XYZZY)   AUDIT(FAIL(READ))
6)   ABCD.TEST3.**    UACC(NONE)      READ(XYZ)       UPDATE(XYZZY)   AUDIT(FAIL(READ))
```

Figure 475. Sample profiles

- ACL entry `XYZZY` makes Profile 2 different from Profile 1.
- ACL entry `QWAS` makes Profile 3 different from Profile 1. AUDIT setting `FAIL(UPDATE)` makes Profile 3 different from Profile 1.
- ACL entries `QWAS` and `XYZZY` make Profile 4 different from Profile 1.
- ACL entries `QWAS` and `XYZZY` make Profile 5 different from Profile 1.
- ACL entries `QWAS` and `XYZZY` make Profile 6 different from profile 1.

When analyzing the preceding profiles, *Report Redundant* simply reports several reasons that five profiles are non-redundant. It does not give any recommendation on how to proceed. The installation might decide to reduce the number of profiles by using methods similar to the following methods.

Method 1

Add ACL entry `XYZZY` to Profile 1 and add ACL entry `QWAS` to Profiles 4, 5, and 6. This would make Profiles 2, 4, 5 and 6 redundant, and Profile 3 almost redundant.

Method 2

Add Profile 3a `ABCD.TEST%.**` like Profile 4 `ABCD.TEST1.**`. This addition would make Profiles 4, 5, and 6 redundant.

When consolidating the profiles, the administrator needs some confirmation that it indeed has the intended effect and that no unintended data sets were affected by this change.

When using Method 2, the process could be:

1. Use `IRRUT200`, to make a copy of the production RACF database for use as Offline RACF environment.
2. On the displays, use the LR line command to see which data sets are covered by a selected profile. Do this for both the System RACF and the Offline RACF database.
3. After defining the new profiles, recreate and analyze the redundancy report.

4. Delete the now redundant profiles and use the LR line command to verify that only the intended resources were affected.

When using Method 1, the analysis is less complex because the approach only increases access by adding entries to access lists. Using this method, there is little chance of negatively impacting the production environment. However, this is a non-preferred solution because it requires granting unnecessary access.

Testing profiles on multiple systems

In another customer environment, the customer wanted to gradually synchronize RACF profiles on three systems. The customer wanted to analyze the effects of adding or changing profiles on all affected systems before actually implementing the changes. RACF Offline provides the command logging facility and the B8REPLAY command to quickly perform those tasks. The following scenario could be implemented:

1. Start RACF Offline.
2. Reset the LOG file.
3. Issue RACF commands to the default Offline RACF database.
4. Switch to an alternative Offline RACF database.
5. Reset the LOG file.
6. Replay the commands from the default LOG.
7. Issue additional commands to verify changed profiles in context.
8. Switch to the third Offline RACF database.
9. Reset the LOG file.
10. Replay the commands from the default LOG.
11. Issue additional commands to verify changed profiles in context.

The following set of commands illustrates the preceding scenario.

```
B8RACF
B8RACFLG RESET
AD 'some.profile'
B8RVARY SELECT(02)
B8RACFLG RESET
B8REPLAY SELECT(01)
LD DA('some.dataset') gen
B8RVARY SELECT(03)
B8RACFLG RESET
B8REPLAY SELECT(01)
LD DA('some.dataset') gen
```

Using an iterative approach, the commands can be refined to have the desired effect in all three environments.

Of course, using prepared batch jobs and submitting the commands to three different target systems is also possible. However, this approach involves one of the following: issuing the commands directly on the production target systems, the use of three test LPARs, or complicated switching of the System RACF database on one test LPAR. Using the process could be implemented in a single batch job or TSO session on a regular test or production system.

System recovery

This application of requires some understanding of the usage of shared disks and the RVARY command to activate or switch RACF databases. Using for recovery purposes significantly reduces system outage time, by reducing the number of IPL's required, and by simplifying the recovery process.

This scenario is based on a multiple LPAR environment with the possibility to share disks between the LPARs. The scenario does not apply to a sysplex

environment, where RACF data sharing has been activated. In the scenario an erroneous RACF command has been issued that prevents the system from IPLing. An example of such a command would be the definition of a PROGRAM profile covering LINKLIB modules. Since OW50327, RACF uses access READ for profile '*' or '**' for SYS1.LINKLIB if a `UACC(NONE)` denies access. However, this APAR does not address situations where another profile (like I*) prevents access, or where the `UACC(READ)` is overruled by an ACL entry (such an ACL entry will not prevent the SYSTEM from starting, but it can have severe impact on major subsystems like VTAM, TCPIP and TSO).

The APAR suggests IPLing with an older (backup) RACF database, and using a sequence of RVARY commands to re-establish the recent RACF database. As soon as the recent RACF database is active, corrective RACF commands can be issued. The older database is used to bypass the IPL problem, and the recent database is quickly re-established to avoid losing profile updates like user password changes.

However, the disadvantage of this recovery scenario is that it requires either some preparation, or complex ad-hoc procedures. For example, you need to prepare an alternative RACF data set name table pointing to the older backup copy. Failing that, the recovery will involve stand-alone utilities to recover the backup copy of the RACF database without destroying the recent RACF database. A single-disk disaster recovery volume would remove the awkwardness of stand-alone utilities in this type of situation.

Instead of IPLing an older (backup) database, it is also possible to use shared disks and to correct the problem. Figure 476 illustrates the environment.

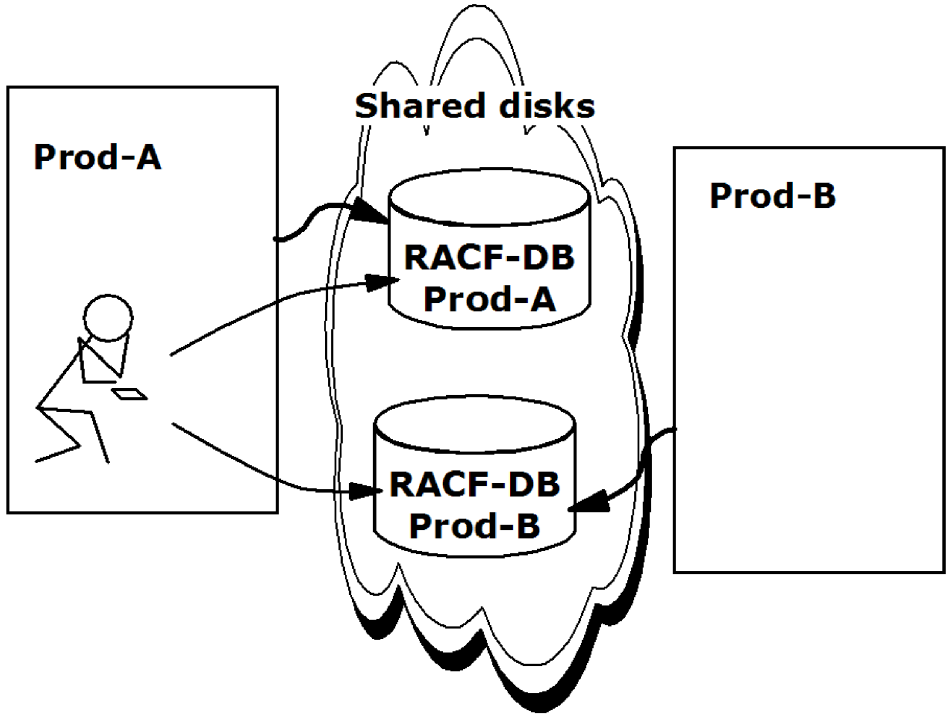


Figure 476. Recovery by multiple LPARs using shared disks

The RACF administrator, who is logged on to the `PROD-A` system can issue RACF commands that are executed on the current system using regular standard RACF

commands. Assume that the troubled system is called PROD-A, and PROD-B has the possibility of sharing disks with PROD-A. In that case, the alternative recovery scenario involves the following steps:

1. Mount the volume with the RACF database of PROD-B on the PROD-A system.
2. Ensure that the RACF database of PROD-B has a different name than that of PROD-A. You might need to rename the database.
3. Issue the B8RACF command for the PROD-B RACF database,
4. Issue the corrective commands and exit B8RACF.
5. Ensure that the RACF database has the proper name for usage on PROD-B. You might need to rename the database.
6. Ensure that the volume is mounted on PROD-B, and IPL PROD-B.

The scenario is less complex and requires less seldom used skills (like use of stand-alone utilities, and multistep RVARY sequences).

Note: An important restriction for this use of is that **all** RACF databases must be primary databases, and that active backup databases are **not** supported. So, after successful recovery of the primary RACF database, copy the primary database over the backup database. Alternatively, you can use to reissue the same recovery commands again to the backup copy of the RACF database.

RACF database switching using RVARY

This section shows the sequence of RVARY and RENAME commands that are used to inactivate the System RACF database, and to activate an Offline RACF database. The advantage of this approach is that executing tasks on the system are not interrupted. However, it is only possible to use these steps if the two RACF databases are sufficiently alike. For instance, the USERID and current GROUP of active tasks should exist in both the *current* System RACF database as well as the *new* System RACF database. If the two databases are dissimilar, results can be unpredictable. Suppose the current RACF databases are:

```
Primary:     SYS1.RACF.PRIM
Backup:      SYS1.RACF.BACK
```

Only one Offline RACF database exists:

```
Offline:     SYS1.RACF.OFFLINE
```

To inactivate the primary RACF database, you can issue the RVARY SWITCH command. This switches the function of the primary RACF database to the backup; the primary database is deactivated. This results in the following situation:

```
Primary:     SYS1.RACF.BACK
Backup:      unused
Offline:     SYS1.RACF.OFFLINE
Inactive:    SYS1.RACF.PRIM
```

The next step in the process involves the RENAME command to make the Offline RACF database take the place of the primary.

```
rename  SYS1.RACF.PRIM     SYS1.RACF.PRIM.SAVE
rename  SYS1.RACF.OFFLINE  SYS1.RACF.PRIM
```

Now, the next set of RVARY commands can be issued to activate the PRIM (ex-OFFLINE) database.

```
rvary  ACTIVE DATASET(SYS1.RACF.PRIM)
rvary  SWITCH
```

The result of the last set of commands is that the PRIM (ex-OFFLINE) database is first activated as the backup database, and then switched to become the primary database. The BACK database, which was in the primary position is inactivated. At this moment the OFFLINE database has become the active primary database.

```
Primary:     SYS1.RACF.PRIM (ex-OFFLINE)
Backup:      unused
Inactive:    SYS1.RACF.PRIM.SAVE
             SYS1.RACF.BACK
```

If you want to create a backup database for the new PRIM database, you should allocate a data set of appropriate size, and run and IRRUT200 or IRRUT400 job. To prevent data loss, rename the existing BACK data set to BACK.SAVE before creating the new BACK data set.

```
rename  SYS1.RACF.BACK     SYS1.RACF.BACK.SAVE
```

After the IRRUTxxx job to create the new BACK database, the situation is as follows:

```
Primary:     SYS1.RACF.PRIM (ex-OFFLINE)
Backup:      unused
Inactive:    SYS1.RACF.PRIM.SAVE
             SYS1.RACF.BACK.SAVE
             SYS1.RACF.BACK
```

The final command to activate the new BACK database is provided in the following example:

```
rvary  ACTIVE DATASET(SYS1.RACF.BACK)
```

resulting in:

```
Primary:     SYS1.RACF.PRIM (ex-OFFLINE)
Backup:      SYS1.RACF.BACK (copy of ex-OFFLINE)
Inactive:    SYS1.RACF.PRIM.SAVE
             SYS1.RACF.BACK.SAVE
```

RACF Offline commands

This chapter documents the RACF Offline commands and parameters. The main command B8RACF has two different types of subcommands. The first type consists of Control commands, the second type consists of the RACF and additional supporting commands.

The Control Commands can be used as part of the B8ROPT installation options module, or as part of the B8RPARM input file. When control commands are executed as part of the B8RPARM input file, authorization to execute the commands is verified using the authorization profiles described in “Security zSecure Admin RACF Offline authorizations” on page 620.

The RACF commands and additional supporting commands can be entered as part of the SYSTSIN stream. In an interactive TSO job, this input stream corresponds to the terminal. Because uses regular TSO services for obtaining command input, it is also possible to redirect command input using CLISTs and REXX execs for example.

The next sections describe the control commands, followed by the RACF and supporting commands.

The B8RACF command and Control commands

The environment is activated using the B8RACF command. This command does not accept any keywords or parameters. Instead, before setting up the environment, and prompting the terminal user for RACF commands, it processes several supporting commands from two different sources. The first set of commands comprises those commands that are set up during installation. These commands are located in the B8ROPT module. The second set of commands is retrieved from the B8RPARM DD-statement. The B8ROPT module is required, and must at a minimum specify the resource class used for profiles. After successful execution of the commands from both sources, the terminal user is prompted to enter RACF commands.

Control commands specified using B8ROPT and B8RPARM

This section describes the syntax and authorization requirements for the Control commands.

RACFDB
Specify the Offline RACF database.

LOGDS
Specify the LOG file.

SMF
Specify the SMF processing options.

END
End the Control commands.

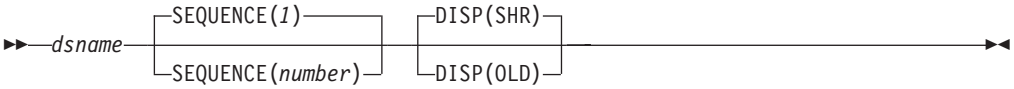
For information about reading the syntax diagrams, see Appendix A, “Reading Syntax Diagrams,” on page 1689.

Specifying the RACF database to be used

The following diagram describes the RACFDB command. The RACFDB command can be issued either as part of the B8ROPT module, as part of the B8RPARM input stream, or in the B8ROPTxx files. In the absence of any RACFDB commands, attempts to use the databases that are preallocated to ddnames INDD1 to INDD*n*.

If your RACF database is physically split into multiple databases, that the number of RACF databases used should match the number of databases specified in your System RACF database range table (ICHRRNG). Also, the System RACF database range table should specify the actual key ranges used for the Offline RACF databases.

RACFDB



The RACFDB command is used to specify which databases to use for this session. Because a RACF database can be physically split into multiple data sets, multiple RACFDB commands can be issued to specify all physical data sets. In that case you should also specify the sequence number. When specifying multiple RACFDB commands, specify the data sets in ascending sequence number order.

dsname
The *dsname* specifies the name of your Offline RACF database. Standard TSO

naming conventions apply. If the data set name does not start with your TSO prefix, enclose the data set name in single quotes unless your TSO profile is set to *noprefix*.

SEQUENCE(number)
The sequence number should match the relative data set number that is used in your RACF range table. If your RACF database is not physically split, you can omit the SEQUENCE keyword. In that case, the default (1) is used.

DISP(disp)
The default disposition of the data set is SHR. That means that other users can concurrently access the same Offline RACF database. Normal RACF serialization applies, so concurrent updates are possible without loss of database integrity. However, serialization does not guard against other types of access to the database. If you want to have exclusive access to this particular RACF database, you can also specify disposition OLD. Although the value NEW is accepted, it is currently ignored, and treated as SHR.

Specifying the LOG file to be used

The following diagram describes the LOGDS command. The LOGDS command can be issued either as part of the B8ROPT module, in the B8RPARM input stream, or in the B8ROPTxx files.

LOGDS

The LOGDS command is used to specify which LOG data set is to be used for this session.

dsname
The *dsname* specifies the name of your LOG data set. Standard TSO naming conventions apply. If the data set name does not start with your TSO prefix, enclose the data set name in single quotes unless your TSO profile has been set to noprefix.

The LOGDS command is intended to be used with the RACFDB command. When using the B8RVARY command to switch the Offline RACF database, you must also switch the corresponding LOG data set. By using this setup, the LOG data set contains all commands that have been issued against a particular Offline RACF database.

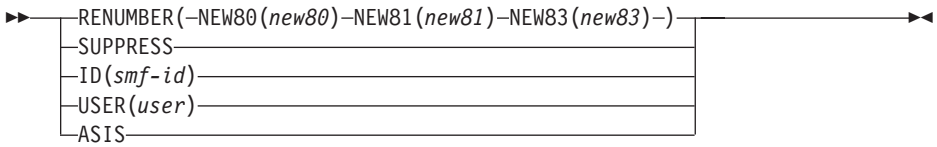
The B8REPLAY command uses the information in the B8ROPTxx file to select the LOG data set (command file) containing the commands to be issued.

Specify SMF processing options

Most of the standard RACF command processors write SMF records during processing. It is almost impossible to distinguish the SMF records written for an update to the Offline RACF database from those records written for an update to the active System RACF database. To enable identification, use the SMF command to mark SMF records as written during a session. Some of the command options apply to all SMF records, while others apply only to the RACF SMF records. The best option is to modify the SMF-ID for the affected records.

Note: See "Auditing" on page 603 for important prerequisites for SMF record processing.

SMF



The SMF command is used to specify how to handle the SMF records created while is active. Several possibilities are provided. To ensure that the relevant SMF records can be identified, include the SMF command in the B8ROPT installation options module. This way, the installation can ensure that the relevant SMF records can be identified. If you do not include the command in the B8ROPT installation options module, no SMF command is issued, and the default action is that all SMF records are left unmodified. This means that the records cannot be distinguished (other than by time of day) from those SMF records that are created as part of regular RACF commands that affect the active system RACF database.

RENUMBER
The renumber keyword indicates that you want the RACF SMF records to be assigned a different record type. The command has three subkeywords to specify the new record types for the three types of RACF SMF records.

NEW80(new80)
The *new80* variable specifies the new SMF record-type to assign the standard RACF type-80 SMF records, while is active. For best results, set this value to *180*.

NEW81(new81)
The *new81* variable specifies the new SMF record-type that is to be assigned to the standard RACF type-81 SMF records, while is active. For best results, set this value to *181*.

NEW83(new83)
The *new83* variable specifies the new SMF record-type that is to be assigned to the standard RACF type-83 SMF records, while is active. For best results, set this value to *183*.

SUPPRESS
The SUPRESS keyword indicates that all SMF records created while the keyword is active are suppressed. Use this option only when you are sure that the RACF commands issued will never affect a RACF database involved in production processes. Example of such usage would be a temporary database used for educational purposes.

ID(smf-id)
The ID keyword indicates that you want to assign a different SMF-ID (System-id) to those SMF records created while is active. The assignment of the new ID applies to all SMF-records. This is the best option to allow these records to be differentiated from records written when other databases are active. The resulting SMF records can be separated easily using the SID(smf-id) control statement for the IFASMFDP and IRRADU00 utilities for example.

USER(user)
Indicates that you want to assign a different USER(*SMF80UID*) value in the RACF command SMF records. The assignment of the new user value applies only to SMF record type 80. This field is usually empty unless the installation has

placed a specific value in the SMF Common Exit Parameter Area (CEPA) using the IEFUJI SMF exit. The value of this field is installation-specific and does not need to represent the RACF `userid`.

ASIS
The ASIS keyword indicates that you do not want to modify any SMF record created while RACF Offline is active. This means that all SMF records generated by the RACF commands for actions against the Offline RACF database cannot be distinguished from those against the System RACF database. Select this option if you are not concerned about any RACF command auditing. Using this keyword makes sense only for preparing or testing on a test partition.

Ending the Control commands

The following diagram describes the END command. The END command is required as the last command in the B8ROPT module. It can also be used to signal the end of the B8RPARM file. In the absence of the END command, processing of the Control commands continues to the end of the B8RPARM file. The EXIT command can be used as alternative to the END command. It performs identical functions.

END

As indicated in the preceding diagram, the END command does not have any keywords or parameters. It indicates the end of the input file.

RACF commands and supporting commands

After successful execution of the Control commands, the terminal user is prompted to enter RACF and supporting commands. These commands can be entered from the terminal, or are read from the SYSTSIN DD-statement when B8RACF is used in batch.

This section describes the syntax of the RACF and supporting commands. For information about reading the syntax diagrams, see Appendix A, “Reading Syntax Diagrams,” on page 1689.

RACF commands

RACF Offline supports most RACF commands in unmodified form. The RVARY, SETROPTS, and RACLINK commands are not supported. Also, RRSF support is explicitly disabled in RACF Offline. Do not use the AT or ONLYAT keywords, both are ignored. Irrespective of the system settings specified using the TARGET operator command, automatic command direction is not performed.

Supporting commands

In addition to the RACF commands, RACF Offline provides additional supporting commands. These commands are summarized in the following table.

Table 269. RACF Offline supporting commands

Command	Description
“**B8RACFLG**” on page 616	Manage the LOG file.
“**B8REPLAY**” on page 617	Reissue RACF commands from a LOG file.
“**B8RVARY**” on page 617	Switch and select Offline RACF database

Table 269. RACF Offline supporting commands (continued)

Command	Description
"**CKGRACF**" on page 618	Run the CKGRACF program.
"**END**" on page 618	End the session.
"**EXEC/EX**" on page 618	Run a REXX EXEC or TSO CLIST.
"**ISPF**" on page 619	Enter ISPF.
"**LOGON**" on page 619	Use authorization of user in Offline RACF database.
"**PROFILE**" on page 620	The TSO PROFILE command.
"**REPORT**" on page 620	Report RACF command usage.
"**TIME**" on page 620	The TSO TIME command.
"**TRACE**" on page 620	Invokes the RACTRACE command. Before using this command, you must install the RACTRACE function. For details, see "**TRACE**" on page 620.

The following sections provided more detailed information about the RACF Offline supporting commands. Commands are presented in alphabetical order.

B8RACFLG: The B8RACFLG command can be used to reset or list the name of the LOG file used to record all RACF commands issued against an Offline RACF database. This command is available in both the B8RACF and the ISPF environment. The command has the following syntax.

B8RACFLG

The B8RACFLG command accepts one keyword, which can have one of the following values.

Open
The OPEN keyword specifies that the LOG file is to be opened. This function is only available if the log data set has been specified using the LOGDS Control command.

Close
The CLOSE keyword specifies that the LOG file is to be closed. This function is only available if the log data set has been specified using the LOGDS Control command.

Reset
The RESET keyword specifies that the LOG file is to be reset. All information recorded up to that point will be overwritten with the new LOG of RACF commands issued.

Flush
The FLUSH keyword specifies that the LOG file is to be flushed. All buffers are written. The LOG file will continue to be used. This function is only available if the log data set has been specified using the LOGDS Control command.

List
The LIST keyword requests display of the data set name for the LOG file currently in use. Figure 477 shows an example of the output.

```
 B8R200A Enter RACF Command or "END"
b8racflg list
 B8R287I Current logfile is BCSC.RACFDS.B8RLOG
 B8R200A Enter RACF Command or "END"
```

Figure 477. B8RACFLG command List option output

B8REPLAY: The B8REPLAY command can be used to reissue the commands saved in a LOG file. The SELECT(xx) parameter on the B8REPLAY command identifies a pre-allocated B8ROPTxx file. That B8ROPTxx file is scanned for the LOGDS statement naming the LOG data set that is to be used. This command is available in both the B8RACF and the ISPF environment. The command has the following syntax:

B8REPLAY

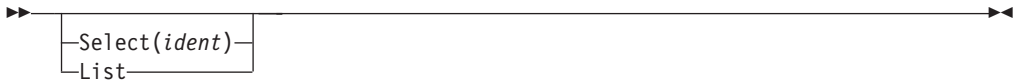
The following keywords and parameters can be used:

Select
The SELECT keyword specifies the B8ROPTxx DD-statement that contains Control commands. The last two characters of the DD-statement are provided by the *ident* value.

ident
The *ident* value is used as the last two characters of the B8ROPTxx DD-statement.

B8RVARY: The B8RVARY command can be used to switch and select the Offline RACF database that is used. It can be issued with a parameter to select a file containing RACFDB, LOGDS, and SMF commands. You can also issue B8RVARY without any parameters. In that case, the terminal user is prompted for confirmation and the Control commands. For the available Control commands, see section "The B8RACF command and Control commands" on page 612. This command is available in both the B8RACF and the ISPF environment. The command has the following syntax:

B8RVARY



The following keywords and parameters can be used:

Select
The SELECT keyword specifies the B8ROPTxx DD-statement that contains Control commands. The last two characters of the DD-statement are provided by the *ident* value.

ident
The *ident* value is used as the last two characters of the B8ROPTxx DD-statement.

List

The LIST keyword requests a display of the Offline RACF databases currently in use. Figure 478 shows an example of the output.

```
 B8R200A Enter RACF Command or "END"
b8rvary list
 B8R246I RACF databases in use
 B8R247I Number   Volume     Dataset
 B8R248I    1     BCSC02     BCSC.RACFDS
 B8R200A Enter RACF Command or "END"
```

Figure 478. B8RVARY command List option output

If you use B8RVARY without any keywords or parameters, an interactive switch of the Offline RACF database is assumed. You are prompted to confirm switching. Following confirmation, you are prompted for additional Control commands (RACFDB, LOGDS, and SMF). This allows for flexible selection of the desired databases and options. Terminate the prompting sequence with the END command.

```
 B8R200A Enter RACF Command or "END"
b8rvary
 B8R232A Confirm switching RACFDB (YES/NO)
yes
 B8R234A Enter B8RVARY subcommand or "END"
racfdb 'bcsc.racfds'
 B8R274I RACF DB to be used is BCSC.RACFDS
 B8R234A Enter B8RVARY subcommand or "END"
logds 'bcsc.racfds.b8rlog'
 B8R268I LOG data set to be used is BCSC.RACFDS.B8RLOG
 B8R234A Enter B8RVARY subcommand or "END"
end
 B8R200A Enter RACF Command or "END"
```

Figure 479. Using the B8RVARY command interactively

CKGRACF: This command invokes the CKGRACF command which allows management of USRDATA fields, other "difficult" fields. For more information on CKGRACF, see Chapter 14, “CKGRACF Command Language,” on page 1499. The authorization to use the CKGRACF functions is obtained from the Offline RACF database.

END: The END command is used to signal the end of the RACF command input stream. In the absence of the END command, processing of RACF commands continues to the end of the SYSTSIN input file. The EXIT command can be used as an alternative to the END command. It performs identical functions. This command is applicable only in the B8RACF environment.

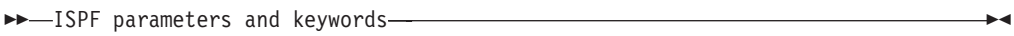
END

The END command does not have any parameters.

EXEC/EX: Execute a REXX EXEC or TSO CLIST. The RACF commands in this file are executed against the Offline RACF database. This command is available in the B8RACF environment, as well as in the ISPF environment.

ISPF: This starts the ISPF full-screen environment. Most of the functions of ISPF use the System RACF database. If RACF commands are issued, using either option-6 or the RACF panels, the Offline RACF database is used. When leaving the ISPF full-screen environment, line-mode B8RACF resumes. This command is applicable only in the B8RACF environment.

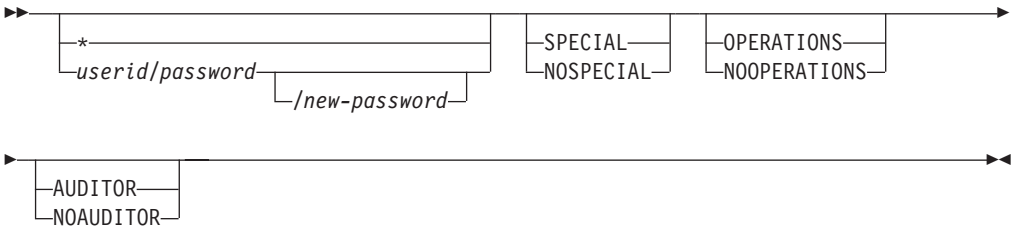
ISPF



The ISPF supporting command for B8RACF accepts the same parameters and keywords as the TSO ISPF command. For more information on these parameters and keywords, see ISPF documentation or the ISPF HELP file.

LOGON: The LOGON command results in using the RACF authorizations of a user in the Offline RACF database. This command is applicable only in the B8RACF environment. The LOGON command has the following syntax:

LOGON



If you enter just the LOGON command without any parameters, the current `userid` is used to LOGON to the Offline RACF database. If you specify a *userid*, you must also specify the password of that userid. If you want to be prompted for the password in non-display mode, end the USERID with a forward slash (/).

If you specify the current password, you can also specify a new password. To be prompted for the new password in non-display mode, end the current password with a forward slash (/).

You can also explicitly specify that you want to logon using your current userid by using an asterisk (*). In that case, any password you specify is ignored.

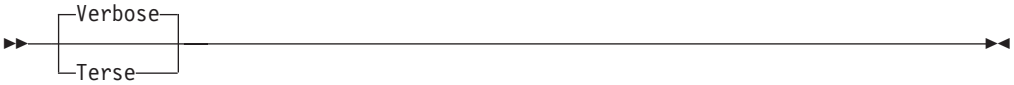
The optional attribute keywords (NO)SPECIAL, (NO)OPERATIONS, and (NO)AUDITOR request that the effective value of the specified attribute is temporarily set or reset after logging on to the Offline RACF database. The value of the attribute in the Offline RACF database itself is not changed. Use of these keywords requires access to the B8R.*attribute.master-racfdb-name* resource in the XFACILITY resource class in the System RACF database. For more information about the required authorization see “Command authorization verification” on page 621.

If you specify one of the optional attribute keywords, you also must specify a value for the userid, including the password, or use an asterisk to logon using your current userid. Password prompting in non-display mode is not supported when using an optional attribute keyword.

PROFILE: This command runs the regular TSO PROFILE command. It can be used for instance to specify the data set prefix or to specify that messages should include a message identifier, or that WTP messages should be shown on the terminal.

REPORT: The REPORT command can be used to print a summary of the RACF commands issued in the current session. The resulting display contains a header, a list of the supported RACF commands including the number of times that the command ended with a particular return code, and a *Total* line showing the total number of commands issued. This command is applicable only in the B8RACF environment.

REPORT



The REPORT command accepts one keyword, which can have the value Verbose or Terse.

Verbose
All supported RACF commands plus a Total line are listed in the command usage report.

Terse
Only those RACF commands that were issued, including a Total line are included in the command usage report. An example display is provided in the following example.

```
 B8R200A Enter RACF Command or "END"
report terse
 B8R450I Command      #rc0     #rc4     #rc8
 B8R451I ALTUSER         1        0        0
 B8R451I LISTUSER        1        0        0
 B8R452I Total           2        0        0
 B8R200A Enter RACF Command or "END"
```

Figure 480. REPORT command Terse option display

TIME: This command runs the regular TSO TIME command.

TRACE: The TRACE command invokes the RACTRACE function that provides Write To Operator (WTO) trace messages of the RACROUTE calls issued by most applications. Before using this command, you must install the RACTRACE function in the appropriate system libraries. You can download this function from the RACF Downloads site accessible at http://www-03.ibm.com/servers/eserver/zseries/zos/racf/goodies.html. The use of the RACTRACE function can result in large amounts of console and syslog messages and is not intended for use by regular users. The authorization to use the RACTRACE functions is obtained from the Offline RACF database.

Security zSecure Admin RACF Offline authorizations

This chapter discusses the Security zSecure Admin RACF Offline resources used to verify authorization to use the B8RACF command and its control commands. When the commands are issued as part of the B8ROPT options module, no authorization check is performed. When the commands are executed as part of the

B8RPARM input file, the user must have sufficient authority to the specified resources. The resources should be covered by profiles in the resource class as specified in the B8ROPT installation options module. (XFACILIT is the default.) Generic profiles are permitted. For any resource that is not covered by a profile, the corresponding function is not permitted.

No matter how the Offline RACF database is specified (using either B8ROPT, B8RPARM, or preallocated), the user must always have UPDATE access to the resource described in "RACFDB." This is verified at the end of parameter processing.

Aside from the resources described in this section, the user should also have sufficient access to standard RACF resources, like UPDATE access to the selected RACF database.

Authorization to use RACF Offline

The authorization to use the B8RACF command, and therefore the authorization to use the Offline RACF environment as provided by Security zSecure Admin RACF Offline is controlled by the following resource.

B8R.RACF.OFFLINE. This resource controls usage of the B8RACF command. The user needs at least READ access to this resource.

Command authorization verification

Some Security zSecure Admin RACF Offline commands and their keywords are controlled using several resources. These resources are described in the following sections.

RACFDB

The RACFDB command has one major parameter: The name of the data set to be used as the Offline RACF database. When using the RACFDB command, the user must have UPDATE access to the resource. If the Offline RACF database is preallocated, Security zSecure Admin RACF Offline verifies the authority to use the allocated database using the same resource during initialization of the Offline RACF environment.

- **B8R.RACFDB.***dsname*

  This resource controls usage of `dsname` as an Offline RACF database. If the Offline RACF database is only used in a non-data sharing environment, the user needs at least UPDATE authority for this resource. If the Offline RACF database has indicators that it is used in a data sharing environment, the user needs at least CONTROL authority for this resource. If no covering profile has been defined, an error message is issued, and the selected database is *not* accepted. A generic profile can be used to protect this resource.

  In addition to this resource that describes the authority to use the selected data set as an Offline RACF database, the user also needs regular UPDATE access to use the selected data set.

SMF

Each of the major keywords of the SMF subcommand is protected by its own resource. If no covering profile has been defined for the specified keyword, the command is rejected.

- **B8R.SMF.ASIS**

  This resource controls use of the ASIS option of the SMF command. The user needs at least UPDATE authority to this resource.

- **B8R.SMF.SUPPRESS**

  This profile controls use of the SUPPRESS option of the SMF command. The user needs at least UPDATE authority to this resource.
- **B8R.SMF.RENUMBER**

  This resource controls use of the RENUMBER option of the SMF command. The user needs at least UPDATE authority to this resource.
- **B8R.SMF.ID**

  This resource controls use of the ID option of the SMF command. The user needs at least UPDATE authority to this profile.
- **B8R.SMF.USER**

  This resource controls use of the USER option of the SMF command. The user needs at least UPDATE authority to this resource.

LOGON

Use of the optional attribute keywords on the LOGON command requires authorization. The following resources are verified:

- B8R.SPECIAL.*master-racfdb-name*
- B8R.OPERATIONS.*master-racfdb-name*
- B8R.AUDITOR.*master-racfdb-name*

The *master-racfdb-name* is the name of the first or only RACF database used in the RACF Offline session. If your RACF database is physically split, it is the database allocated with sequence number 1. If your RACF database is not physically split, it is just the name of the RACF database. An example resource name is

```
B8R.SPECIAL.SYS1.RACFDS
```

The required access level is UPDATE. If you have insufficient access, or if no profile is found, an ICH408I violation message is issued by RACF, an error message is issued by RACF Offline, and the effective value of the requested attribute is not changed.

Chapter 9. Merge Usage Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•			

Use the Security zSecure MERGE command to merge RACF databases from multiple systems or to prepare for the RACF Remote Sharing Facility (RRSF). The `MERGE` operation analyzes RACF databases and creates the commands required for merging the data. You can use the MERGE command in combination with other zSecure functions to simplify operations like the following:

- List and compare multiple RACF databases (either from different system images, or the same system image at different times).
- Identify differences between databases on different systems.
- Synchronize databases.
- Merge one database into another while resolving definition conflicts.
- Rename profiles.

In order to synchronize data from different RACF databases, you must perform the following tasks:

- Collect profile data from multiple RACF databases.
- Analyze the data to determine the content differences between databases.
- Run RACF commands to reconcile the differences in data.

Security zSecure helps you perform these steps. The program reads profiles from different databases, compares the profiles, and produces reports for identifying differences in the data. It also creates the RACF commands required to merge the data. You can analyze the reports and the RACF commands generated before running the commands. You can also modify the commands if necessary. When you finish your analysis, you can run the RACF commands to merge the information from the source database into the current database. This process relies on the following commands:

- The `SUMMARY` command compares the databases and list the differences.
- The `MERGE` command generates the commands to merge database content and synchronize the data.

For information more information about merging RACF database content, see the following topics:

Listing and comparing profiles from more than one RACF database

Security zSecure uses the live RACF database or the data sources specified on the Setup - Files panel (option **SE.1**).

The CARLa command for reading from a RACF database or unload copies of the database is ALLOCATE (ALLOC). Because the RACF database does not contain system identification, you must include the COMPLEX keyword on the ALLOC command to specify an identifier for each database. The COMPLEX value is a one- to eight-character name required to distinguish which complex the records were read from. The following CARLa commands identify data sets from two different systems:

```
ALLOC DSN='SYS1.ZSECUR.SYSA.UNLOAD' TYPE=UNLOAD COMPLEX=ALPHA
ALLOC DSN='SYS1.ZSECUR.SYSB.UNLOAD' TYPE=UNLOAD COMPLEX=BRAVO
```

You can create these statements using either of the following methods:

- Generate them automatically based on the set of input files selected, including the COMPLEX assigned to the input data sets.
- Use the Command option (**CO.C**) to run the commands yourself.
- Specify the statements in the SYSIN statement of a batch job.

List profiles from both systems

Use the SELECT and LIST commands to list the profiles from both systems as shown in the following example.

```
NEWLIST TYPE=RACF TITLE='SYS1 profiles from both systems'
  SELECT CLASS=DATASET SEG=BASE QUAL=SYS1 COMPLEX=(ALPHA,BRAVO)
  SORTLIST KEY COMPLEX UACC ACL
```

Running this command produces the following results:

```
P R O F I L E   L I S T I N G    1 Aug 1996 06:30
SYS1 profiles from both systems

Profile key         Complex  UACC    User     Access  ACL Id
SYS1.*.**           BRAVO    NONE    IBMUSER  ALTER   IBMUSER
SYS1.**             ALPHA    NONE
SYS1.**             BRAVO    NONE    IBMUSER  ALTER   IBMUSER
SYS1.**.VTAMLST     ALPHA    NONE    -group-  UPDATE  SYSBASE
                                     -group-  UPDATE  SYSNET
SYS1.**.VTAMLST     BRAVO    NONE    -group-  UPDATE  SYSBASE
                                     -group-  UPDATE  SYSNET
                                     SYSCNM   READ    SYSCNM
```

```
P R O F I L E   L I S T I N G   12 Jun 2010 21:38
SYS1 PROFILES FROM BOTH SYSTEMS

Profile key         Complex  UACC    User     Access  ACL id   When
AMVQRK01.191        ZVICOM53 NONE    AMVQRK01 ALTER   AMVQRK01
AMVQRK02.191        ZVICOM53 NONE    AMVQRK02 ALTER   AMVQRK02
AMVQRK03.191        ZVICOM53 NONE    AMVQRK03 ALTER   AMVQRK03
AMVQRK04.191        ZVICOM53 NONE    AMVQRK04 ALTER   AMVQRK04
AFEROIE.191         PTHVM8   NONE    AFEROIE  ALTER   AFEROIE
                                     MAINT    ALTER   MAINT
ATIGTEL.191         PTHVM8   READ    ATIGTEL  ALTER   ATIGTEL
                                     MAINT    CONTROL MAINT
                                     -group-  READ    FAULTTXT
ATIGTEL.192         PTHVM8   READ    ATIGTEL  ALTER   ATIGTEL
                                     MAINT    CONTROL MAINT
                                     ATIGTE2  CONTROL ATIGTE2
```

Determining which system contains a profile

Use the SUMMARY command to determine the system that a profile comes from as shown in the following example:

```
NEWLIST TYPE=RACF TITLE='SYS1 profiles from both systems'
  DEFINE INA BOOLEAN WHERE COMPLEX=ALPHA
  DEFINE INB BOOLEAN WHERE COMPLEX=BRAVO
  SELECT CLASS=DATASET SEGMENT=BASE QUAL=SYS1 COMPLEX=(ALPHA,BRAVO)
  SUMMARY KEY INA INB
```

Running this command produces the following results:

```
P R O F I L E   L I S T I N G    1 Aug 1996 06:30
SYS1 profiles from both systems

Profile key                    INA INB
SYS1.*.**                      No  Yes
SYS1.**                        Yes Yes
SYS1.**.VTAMLST                Yes Yes
```

This report does not show each profile record, but only one line for each profile key and the indication which profiles exist in database *ALPHA*, *BRAVO* or both.

Locating profiles that exist only on one system

You can adapt the SUMMARY command to find profiles that exist only on one system. To list this information, you specify commands to count the profiles located for each profile key value and only list the key value if less than two profiles have this key. The following code sample shows how to locate these profiles.

```
NEWLIST TYPE=RACF TITLE='SYS1 profiles from both systems'
  DEFINE INA BOOLEAN WHERE COMPLEX=ALPHA
  DEFINE INB BOOLEAN WHERE COMPLEX=BRAVO
  SELECT CLASS=DATASET SEGMENT=BASE QUAL=SYS1 COMPLEX=(ALPHA,BRAVO)
  SUMMARY KEY INA INB COUNT(NONDISPLAY,<2)
```

Running this command produces the following results, which show only profiles that are on one system:

```
P R O F I L E   L I S T I N G    1 Aug 1996 06:30
Profile differences between two systems

Profile key                    INA INB
SYS1.*.**                      No  Yes
SYS1.TEST.**                   Yes No
```

Listing and comparing profiles from a current and an old database

Whenever a job fails, end users are quick to blame RACF. The most frequent question is: "What was changed since the last time I ran this job?" With a few simple CARLa statements, Security zSecure shows which profiles were added or deleted.

By allocating multiple RACF data sources from the same system, you can determine which profiles were added to the system as shown in the following example.

This example is based on the following configuration:

- A GDG of unloaded databases created on a daily basis
- Label the two most recent unloaded databases as OLD and CURRENT.

By allocating multiple RACF data sources from the same system, you can determine which profiles were added to the system as shown in the following example. To accomplish this task, use a current copy of the UNLOAD file or create one. Then, restore from backup an UNLOAD file from a time suitable for determining any changes.

The following CARLa commands list profiles from both databases:

```
ALLOC DSN='SYS1.ZSECUR.UNLOAD(-1)' TYPE=UNLOAD COMPLEX=OLD
ALLOC DSN='SYS1.ZSECUR.UNLOAD(0)' TYPE=UNLOAD COMPLEX=CURRENT

NEWLIST TYPE=RACF TITLE='SYS1 profiles yesterday and today'
  SELECT CLASS=DATASET SEG=BASE QUAL=SYS1 COMPLEX=(OLD,CURRENT)
  SORTLIST KEY COMPLEX UACC ACL
```

Running this command produces the following results:

```
P R O F I L E   L I S T I N G    1 Aug 1996 06:30
SYS1 profiles yesterday and today

Profile key         Complex  UACC    User     Access  ACL Id
SYS1.*.**           CURRENT  NONE    IBMUSER  ALTER   IBMUSER
SYS1.**             OLD      NONE
SYS1.**             CURRENT  NONE    IBMUSER  ALTER   IBMUSER
SYS1.**.VTAMLST     OLD      NONE    -group-  UPDATE  SYSBASE
                                     -group-  UPDATE  SYSNET
SYS1.**.VTAMLST     CURRENT  NONE    -group-  UPDATE  SYSBASE
                                     -group-  UPDATE  SYSNET
                                     SYSCNM   READ    SYSCNM
```

The SUMMARY command identifies profiles added or deleted since yesterday by requesting those profiles that only exist in one database:

```
NEWLIST TYPE=RACF TITLE='Profiles added and deleted'
  DEFINE ADDED('Add',HDR$BLANK) BOOLEAN WHERE COMPLEX=CURRENT
  DEFINE DELETED('Del',HDR$BLANK) BOOLEAN WHERE COMPLEX=OLD
  SELECT SEGMENT=BASE COMPLEX=(OLD,CURRENT)
  SUMMARY CLASS KEY ADDED DELETED COUNT(NONDISPLAY,<2)
```

Running this command produces the following results:

```
P R O F I L E   L I S T I N G    1 Aug 1996 06:30
Profiles added and deleted

Class    Profile key        Add  Del
DATASET  NEWUSER.**         Add
DATASET  SYS1.*.**          Add
DATASET  SYS1.TEST.**            Del
TAPEVOL  006269             Add
TAPEVOL  006765             Add
USER     NEWUSER            Add
P R O F I L E   L I S T I N G   28 Apr 2010 05:48
PROFILES ADDED AND DELETED

Class    Profile key          ADD DEL
ACCTNUM  FAKECDT.ACCTNUM.126  ADD
APPCLU   FAKECDT.APPCLU.118   ADD
APPCSERV FAKECDT.APPCSERV.84  ADD
SURROGAT LOGONBY.CHKQUEUE     DEL
USER     CHKQUEUE             ADD
USER     CRMBKW1              ADD
VMBATCH  FAKE015              ADD
```

You can use the SORTLIST and SUMMARY commands to combine the profile results from up to 32 complexes.

Merging a database

The MERGE command compares two systems and generates RACF commands to add and modify profiles on one of the systems. The MERGE command is available under zSecure Admin and Audit and zSecure Admin. It does not work if you only use zSecure Audit.

The MERGE command uses a current or main database (CURRENT or MAIN) and a source database (MERGESOURCE or MERGE. The current database receives the profiles copied from the source database. Usually the MERGE command runs on the system with the current database and source database is an unloaded RACF database from another (remote) system.

The merge process produces a list of RACF commands in the CKRCMD file. These commands perform add, delete, and modify actions to merge the content from the source database into the current databases so the databases are approximately the same. You can allocate separate files for different types of commands using the FUNCTION parameter on the ALLOC statement. This parameter specifies what type of commands are written to the file:

TYPE=CKRCMD FUNCTION=MAIN
If this function is specified, the CKRCMD file receives commands that can be run on the system with the current database. This file mostly contains the commands that *add* profiles and entries to the database.

TYPE=CKRCMD FUNCTION=MERGE
Receives commands that can be run on the system with the source database (MERGESOURCE). This file mostly contains the commands to *delete* all profiles are already present in the current system or profiles that were successfully merged. Use the MERGE function to *move* profiles between databases.

If you are not interested in the commands generated to one or both files, you can leave out the ALLOC commands. If no ALLOC command is specified, the program issues the CKR0696 message which you can ignore.

The following sample shows the basic commands to run the MERGE process:

```
ALLOC DSN='SYS1.ZSECUR.SYSA.UNLOAD' TYPE=UNLOAD FUNCTION=MAIN
ALLOC DSN='SYS1.ZSECUR.SYSB.UNLOAD' TYPE=UNLOAD FUNCTION=MERGE
ALLOC DD=CKRCMD TYPE=CKRCMD FUNCTION=MAIN
MERGE
ENDMERGE
```

Running these commands generates RACF commands in the file CKRCMD to add all users, groups, and applications that are currently defined on *SYSB* into *SYSA*.

Because the SETUP application does not support the FUNCTION parameter, you must enter ALLOC commands for the FUNCTION=MERGE data sets using the Security zSecure Command option **CO.C** or in the SYSIN of a batch job.

Note: You cannot MERGE databases accessed by the zSecure network. However, you can MERGE remote UNLOAD files.

Because MERGE uses a lot of virtual storage, it is more efficient to run this function primarily using batch jobs. To create the batch job, do the following:

1. From the Main menu, select the Command option (**CO.C** to open the Command panel.
2. In the entry fields, type the allocation commands for the merge process:

```
ALLOC DSN='SYS1.ZSECUR.SYSA.UNLOAD' TYPE=UNLOAD FUNCTION=MAIN
ALLOC DSN='SYS1.ZSECUR.SYSB.UNLOAD' TYPE=UNLOAD FUNCTION=MERGE
ALLOC DD=CKRCMD TYPE=CKRCMD FUNCTION=MAIN
MERGE
ENDMERGE
```

3. Type SUBMIT on the command line to generate the batch job.
4. From the SUBMIT option panel, you can edit and create the batch job:
   - Select option 2 to edit the generated JCL.
   - Type CREATE on the command line. Then, press **Enter** to save the JCL to an existing work data set.
5. Use the program you created as the base for creating the MERGE batch application.

Note: Member C2RJMALL in the SCKRSAMP library contains the basic MERGE commands. This job is documented in "IBM Security zSecure jobs" on page 699.

Cleaning up security databases

The MERGE command does not run successfully if either of the RACF databases has any serious internal inconsistencies. To start with clean data, run the VERIFY PERMIT,CONNECT command on each database. Then, run the commands generated by the VERIFY operation to clean up the database.

VERIFY PERMIT, CONNECT checks each database for references to undefined IDs, such as groups and user IDs on access lists or in OWNER or NOTIFY fields. These orphaned IDs are caused when IDs are removed from the RACF database without first running IRRUT100. Using Security zSecure to manage your RACF database prevents such inconsistencies.

Resolving inconsistencies

Performing a merge usually results in messages detailing inconsistencies between the two databases. You can use the following information to resolve inconsistence and differences in the databases.

Because conflicts are likely between the two databases, MERGERULE commands are placed between the MERGE and ENDMERGE commands. These rules specify which profiles have precedence. For example, to ensure that profiles in current database have precedence over profiles in the source database specify the following statement:

```
MERGERULE DEFAULT AUTHORITY=CURRENT
```

The current database value is used whenever a user authority differs from the source database. This simplistic approach can cause failed jobs due to insufficient authority. To prevent this problem, you can specify a statement that assigns the higher authority level to an ID that has different values in the current and source databases:

```
MERGERULE DEFAULT AUTHORITY=HIGH
```

For example, if this statement is present, the merge process assigns the UPDATE access to a user ID when the same user has READ access in one system and UPDATE access in the other.

You can specify the MERGERULE command for each user or group in the source database.

```
MERGERULE SOURCEID=PROD AUTHORITY=HIGH
MERGERULE SOURCEID=TEST AUTHORITY=LOW
```

If no MERGERULE applies to an ID, any conflicts in authority for the ID are flagged in the SYSPRINT. You must resolve any conflicts before the commands are generated.

You can use the following statement to specify authority per general resource class:

```
MERGERULE SOURCECLASS=FACILITY AUTHORITY=HIGH
```

Profiles also contain informational fields which can be useful for reporting. You can control the content merging for these fields using the following statement:

```
MERGERULE DEFAULT DATA=CURRENT
```

This statement indicates that the contents of fields in the current database are to be kept even if the contents are different from the source database. This processing applies to fields like the default group, programmer name, and installation data as well as the TSO segment.

If you do not specify MERGERULE commands, Security zSecure flags discrepancies in authority and incompatible data fields and stops processing.

Selecting profiles

Specify SELECT commands in the MERGE-ENDMERGE block to identify those IDs from the source database that must be copied into the current database. Only fields in the BASE segments of all profile classes are available for selection processing. The non-BASE segments like the CICS, DFP, and TSO application segments are automatically copied without any selection. This behavior means that these application segments are automatically processed during the merge, but it also means that you cannot use the existence of a segment as a selection criterion for all CICS or TSO users.

The following code sample shows how to copy the group *PROD* and all its user IDs:

```
MERGE
  SELECT CLASS=GROUP KEY=PROD
  SELECT CLASS=USER OWNER=PROD
  SELECT CLASS=(DATASET,GENERAL),
         (OWNER=PROD OR OWNER:OWNER=PROD OR QUAL=PROD)
ENDMERGE
```

These normal CARLa SELECT commands:

1. Select the group *PROD*, and all users who are directly owned by *PROD*.
2. Select all data set and general resource profiles with the following characteristics:
   - owned directly or indirectly by *PROD*
   - have a dsname that starts with *PROD*

The same techniques used in your CARLa reports work here.

Running these commands only generates commands to connect the users it copied to the group *PROD*. To connect the *PROD* users to all of the groups that they were connected to when the groups exist in the current database, add the following MERGERULE command:

```
MERGERULE DEFAULT CONNECT=IFUSER
```

This command copies all *connects* for users that were selected in the MERGE block. This merge rule is only an appropriate choice when identically named groups in the current and source database have the same function.

Renaming IDs

Use the MERGERULE RENAME operand to generate new users and groups in the current database with the same characteristics as an ID in the source database. Using this operand helps when different naming conventions are used in each of the two databases and profile names must be converted during the database merge.

Renaming can also be helpful when two groups have the same name but perform different functions in each database.

If you only want to copy and rename a single group, you can specify a SELECT and a MERGERULE RENAME command:

```
MERGE
  SELECT KEY=PROD
  MERGERULE SOURCEID=PROD RENAME=APPL
  MERGERULE DEFAULT AUTHORITY=MERGESOURCE DATA=MERGESOURCE
  MERGERULE DEFAULT CONNECT=IFUSER
ENDMERGE
```

When you allocate the same RACF data source as CURRENT and MERGESOURCE, you can rename a group or users within your current database.

Merging groups

You can use the MERGERULE RENAME operand to merge a group into an existing group. This is achieved by excluding the target group from the MERGESOURCE and renaming the source group as shown in the following example:

```
MERGE
  EXCLUDE KEY=APPL
  MERGERULE SOURCEID=PROD RENAME=APPL
  MERGERULE DEFAULT AUTHORITY=MERGESOURCE DATA=MERGESOURCE
ENDMERGE
```

Running these statements generates the commands to add all users in *PROD* to *APPL* when they were not already connected.

When you allocate the same RACF data source as CURRENT and MERGESOURCE, you can merge a group within your current database.

Note: Member C2RJMGRP in the SCKRSAMP library demonstrates this technique. This job is documented in "IBM Security zSecure jobs" on page 699.

Synchronizing passwords

Merge generates CKGRACF commands to set some statistical fields. This functionality can be useful for password synchronization because the commands generated can prevent users from being unduly revoked for inactivity. These commands are created when CKGRACF=YES is specified, which is the default setting. The following guidelines determine how the fields are set by the merge process:

- For a user ID that is present only in the source database, the merge creates a command to set the following fields for the user ID: `LJDATE`, `REVOKECT`, `PASSWORD`, and `PASSDATE`. These fields are set only if they are present.
- The `PASSWORD` is set even if the user ID is not set for password checking.
- If `LJDATE` is set, `LJTIME` is also set.
- If a user ID is present in both databases and the `PASSDATE` in the source database is the most recent one, a command is generated to set `PASSDATE` and `PASSWORD`. Otherwise, if the `PASSDATE` equals zero–indicating a password reset, the `LJDATE` determines whether a `PASSWORD` set command is created.
- If the `PASSWORD` is set for a user ID present in both databases, the command sets `REVOKECT` as well.
- If the `LJDATE` in the source database is the more recent, the command also sets the `LJDATE` and `LJTIME` values.
- CKGRACF commands to set `PASSWORD`, `REVOKECT` and `PASSDATE` are only generated if the zSecure data source is not an unload data set. If the data source is unloaded data, the commands cannot be generated to set password values because unload data does not contain passwords.

Important: If you want to merge password changes, verify that the current database and the source database use the same method for encrypting passwords. The merge process does not check the encryption. If the encryption method is not the same, users can end up with invalid passwords as a result of the merge.

Using MERGE to identify changes in RACF

When we interpret the current database as *yesterday's database* and the source as *today's database*, then `MERGE` can be used to generate commands to make yesterday's database look more like today's. Of course, any interval could be applied, a week or a month for example. zSecure provides the `C2RJMSYN` job to perform the process of merging changes from the current database back to the old database. For information about this procedure and other zSecure jobs and procedures, see Chapter 11, "Calling zSecure," on page 689. The process is complicated because the merge process does not generate both RACF commands to delete profiles from a database and RACF commands to add profiles to that database at the same time.

Note: Like other merge applications, the reporting application also requires that both databases are internally consistent. Security zSecure provides the tools to fix internal problems in a RACF database and maintain consistency between the databases. See "Resolving inconsistencies" on page 628.

You can also use the MERGE NEWLIST function to create custom reports for the MERGE function. You can use this feature to produce regular reports of all changes made to the RACF database or to produce reports on specific profiles if you are trying to understand and document the decisions made during merge processing.

The following code produces a report that shows all fields changes where the current value is different than the source value value or where either value is missing. For every change, the resulting report shows the profile, the field name, the old value and the new value.

```
newlist type=merge title='Fields changed'
  s exists(field) and (cur_value<<>>src_value,
                       or (missing(cur_value) and exists(src_value)),
                       or (exists(cur_value) and missing(src_value)))
  sortlist class profile(26) field,
         cur_value("Old value") src_value("New value")
```

Running this code produces the following results:

```
 D A T A B A S E   M E R G E   R E P O R T    1 Feb 1998 15:33
FIELDS CHANGED

Class    Profile                  Field    OLD VALUE         NEW VALUE
DATASET  C##A.A.*.TEXT            ACL                        C##B(READ)
DATASET  C##A.A.*.TEXT            ACL                        C##CSEL(READ)
DATASET  C##A.A.*.TEXT            ACL      C##A(ALTER)       C##A(READ)
DATASET  C##A.A.*.TEXT            ACL      C##AINT(ALTER)    C##AINT(READ)
DATASET  C##A.A.*.TEXT            ACL      C##BERT(ALTER)    C##BERT(READ)
DATASET  C##A.A.*.TEXT            OWNER    C##B              C##A
```

Note: Member C2RJMDIF in the SCKRSAMP library demonstrates this technique. This job is documented in "IBM Security zSecure jobs" on page 699.

Background

The Security zSecure data base merge functions can be used to merge two RACF data bases. The basic description of a data base merge is as follows:

- The process uses two RACF databases, a source database (SOURCE) and a current database (CURRENT).
- Both databases are read. Selected profiles from the source database are created on the current database.
- You can specify rules to indicate how to resolve problems that occur during merge processing due to differences in the definitions in the two databases.
- The results of the merge process are found in the merge reports and the CKRCMD file that contains the generated RACF commands and optional CKGRACF commands.

  You must always allocate the CKRCMD file for running the commands on the system for the current database. The RACF commands recreate the selected profiles that were copied from the source database.

  The optional MERGE reports describe the decisions made during the merge process. You can customize these reports for your environment.

For more information about how merge processing works, see the following topics:

- "The merge process"
- "The decision-making process" on page 633
- "RACF command processing order in MERGE commands" on page 634

The merge process

This topic describes the implementation of the merge process, in so far as is required to understand the merge in/out commands and merge results. It can be skipped safely when you are reading this manual for the first time.

The merge process is split into a number of successive steps. Each step must succeed for the next step to be run. The MERGE steps are:

1. Check for SETROPTS conflicts.

   The SETROPTS settings for both data bases are compared. If conflicts exist that make it impossible to transfer profiles, the merge process stops.
2. Check for user/group conflicts, check commands.

   During this step, the selected user and group IDs from the source data base are checked against the current data base. The MERGE commands are verified with the data base contents.
3. Determine superior groups.

   During this step, the new superior group for each group transferred or merged is determined.
4. Determine ownership for users and groups.

   During this step, the new owner for each user/group transferred or merged is determined.
5. Merge user-group connections.

   During this step, the new user-group connections and the connect attributes (such as group-special) are determined.
6. Determine default groups.

   During this step, the new default-group for each user is determined.
7. Determine owners for data set profiles and general resource profiles.

   During this step, the owner for each profile is determined.
8. Copy/merge ACL entries of data set and general resource profiles.

   During this step, the profile access lists are merged.
9. Merge remaining user/group/data set/general resource profile attributes.

   During this step, a decision is made on how to copy all other attributes. The decisions are made separately for security-related attributes and non-security-related attributes.
10. Generate RACF commands.

The decision-making process

During each step, the merge process compares selected source profiles with the current data base and tries to resolve any differences. The `MERGERULE` statements specified in the input commands help resolve errors or conflicts in the merge processing. The processing for security-related fields is different from the processing for non-security related fields. Whenever a decision must be made, the following guidelines are used to determine how to merge content:

1. Check for a specific `MERGERULE` command for this profile.

   When determining superior groups in step 3, a `MERGERULE SUPGROUP` command for this group is honored.
2. For security-related fields, check for a `MERGERULE AUTHORITY` command for this profile.

   When a user has a `group-SPECIAL` attribute on the source system but not on the current system, the presence of a `MERGERULE AUTHORITY(SOURCE)` statement for the user determines that the source attribute value `group-SPECIAL` is assigned to the user after the merge.
3. For security-related fields, check for a global `MERGERULE AUTHORITY` command.

   When a user has a `group-SPECIAL` attribute on the source system but not on the current system and no `MERGERULE AUTHORITY` was specified for the user or

group, the presence of a global MERGERULE AUTHORITY(CURRENT) statement determines that the user is not group-SPECIAL after the merge.

4. For non-security (data) fields, check for a MERGERULE DATA command for this profile.

   When a data set profile has owner GROUP1 on the source system and owner GROUP2 on the current system, the presence of a MERGERULE DATA(CURRENT) statement for the high-level qualifier of the data set profile determines that the owner is GROUP2 after the merge.

5. For non-security (data) fields, check for a global MERGERULE DATA command.

   When a data set profile has owner GROUP1 on the source system and owner GROUP2 on the current system and no MERGERULE DATA was specified for the high-level qualifier, a global MERGERULE DATA(SOURCE) would determine that the owner is GROUP1 after the merge.

6. Check for a built-in fallback.

   This check is highly dependent on the merge step. In most cases, this system selects a reasonable default.

7. If all else fails, issue an error message.

RACF command processing order in MERGE commands

The data base merge functions create commands in the following order:

1. Create or change profiles in the SECDATA and SECLABEL classes. These profiles include: Security level, security category, and security-label related profiles.
2. Generate all groups, top-down. For groups owned by a user that does not yet exist, IBMUSER is used temporarily. The owner is corrected in the processing for step 4.
3. Generate all users, in any order. For profiles owned by a user ID that does not exist, IBMUSER is used temporarily. The user is corrected in the processing for step 4.
4. Fix-up the owners for the groups, and users. Assign the correct user for users and groups that use IBMUSER.
5. Create and alter user group connections.
6. Change default groups for existing users, where necessary.
7. Create and alter general resource profiles in the PROGRAM, JESINPUT, APPCPORT, CONSOLE, TERMINAL, and TAPEVOL classes. After these have been defined, conditional access list entries and TVTOC entries can be created.
8. Create and alter data set profiles. After each ADDSD or ALTDSD action, PERMIT commands are issued to create or alter the access list and conditional access list.
9. Create and alter general resource profiles. After each RDEFINE or RALTER action, PERMIT commands are issued to create or alter the access list and conditional access list.

Frequently Asked Questions

For more information about the merge process, see the following topics:

1. “Which users and groups are merged?” on page 635
2. “Who performs the merge?” on page 635
3. “How do renames work?” on page 635
4. “What is DATA and AUTHORITY?” on page 636
5. “How do I check the results?” on page 636

Which users and groups are merged?

The merge process uses SELECT and EXCLUDE statements within the MERGE/ENDMERGE block to select profiles from the source data base. All selected profiles are merged with the current data base. The following processing behavior applies to SELECT commands:

- If no SELECT statement is specified, all profiles are selected.
- Non-RDS CONNECT profiles are selected automatically; the SELECT and EXCLUDE commands are not applied to these profiles.
- For an RDS, profiles are selected if their BASE segment is selected. If you select using fields from non-base segments, selection does not work.

Merging profiles does not always generate RACF commands. For example, no RACF command is created if group SYSCTLG is identical in the source and current data bases.

Who performs the merge?

Any user who has unrestricted access to the source and current data base or unload files can perform the database merge using Security zSecure. The product generates commands that are user-independent.

A system SPECIAL user with the AUDITOR attribute must run the resulting commands because audit attributes are also set. The RACF commands generated by the merge remove the user ID that generated the merge commands from the profiles and access lists created, where appropriate. This step prevents unintended ALTER access list entries.

How do renames work?

Within the MERGE/ENDMERGE block, you can specify MERGERULE SOURCEID RENAME statements. These statements cause a specific high-level qualifier to be renamed. This topic explains how that works.

Each user or group ID for which a RENAME is specified is merged using the new name. In all places where the source database is compared to the current database, the renamed value of the source ID is used. For example, if you rename the source ID CICSUSER to DB2USER, the merge process always compares the source ID CICSUSER to the current ID DB2USER. This value is used even if the current data base contains an ID called CICSUSER. If source group CICSGRP has owner CICSUSER, the merge process merges the group as if the owner was DB2USER.

The rename action applies in the following contexts

- The user or group ID.
- All data set profiles with a high-level qualifier equal to the specified ID.
- All references to the user or group ID: user-group connections, superior groups, subgroups, default-groups, owners, access list entries, notify fields.

The following restrictions apply to rename actions:

- Renames do not apply to general-resource profile names in the current release. They do apply to access list entries of these profiles.
- The merge process requires a one-to-one correspondence of source and current IDs. This requirement means that if you rename a source ID to a name existing in the current database, the latter ID might not be selected to be merged. Similarly, you cannot rename two source IDs to the same name during one merge run.

What is DATA and AUTHORITY?

Use the MERGERULE commands to specify DATA and AUTHORITY rules. Use the following rule of thumb to clarify when DATA applies and when AUTHORITY applies.

> If a field has values that can be compared as high and low (including some lists) and the settings are used for RACF, then AUTHORITY applies. Otherwise, DATA applies.

For example, if a field has text values like `OWNER` or `SUPGROUP`, the choice is typically between the source value and the current value, so DATA applies. If a field has numeric or logical values, but it is used for an external product like TSO region size, DATA applies.

AUTHORITY applies to RACF-specific logical values as described in Table 270.

Table 270. Use of AUTHORITY setting in merge processing

Field	Description
Access lists	The AUTHORITY setting determines both which access list entries are merged, and the access value used.
Connect attributes	The AUTHORITY setting determines the values of the following connect-attributes: • Authority, `JOIN` or `USE` for example • UACC • Group attributes: group-special, group-operations, group-auditor, group-ADSP, group-GRPACC, and group-revoke status.
Other attributes	The AUTHORITY settings is used for the special, operations, and auditor attributes; the revoke status; the UACC; and the security level.

How do I check the results?

The results of the merge process consist of RACF commands in the `CKRCMD` files and merge reports (`MERGE NEWLIST`).

You can check how a specific profile is processed by browsing the `CKRCMD` file which contains the RACF commands for altering the profile.

If your merge results look strange or cause undesirable effects in the RACF database, you can review the merge reports. These reports provide information about what commands were generated and run during merge processing. The reports can help you understand the decisions made for each profile. You can use the SELECT command to filter the merge reports to review data for specific resources. The following list presents some of the `SELECT` options that are useful for researching specific profiles:

- Use the SRC_PROFILE, CUR_PROFILE, and PROFILE fields for selecting specific profiles.
- Use the PASS and FIELD fields for selecting information about decisions made during a specific pass or for a specific field.
- The SRC_VALUE, CUR_VALUE, and NEW_VALUE fields describe what happened to the values for a specific field. You can pinpoint when changes were made by using the field-field compare operators, SRC_VALUE==NEW_VALUE or CUR_VALUE<<>>NEW_VALUE, for example.

For more information about the SELECT statement and options, see "MERGE: RACF Database Merge" on page 1101

How do I fix errors?

During the merge process, you can encounter two types of problems:

- Errors generated during the merge process, which cause the merge to stop.
- Undesirable results after merging the databases.

You can resolve both types of problems by adding or changing the MERGERULE commands.

For errors during the merge process, study the error message and the *IBM Security zSecure: Messages Guide*. These errors typically occur when the merge process has no value at all or cannot choose between two values, two owners for example.

You can resolve conflicts between two values by adding a MERGERULE DATA or a MERGERULE AUTHORITY command. To apply these commands to one or more specific profiles, specify a MERGERULE SOURCEID or MERGERULE SOURCECLASS. To apply a default for all profiles, use a MERGERULE DEFAULT command.

If no value can be found, either specify a superior group or owner using a MERGERULE SOURCEID command, or add to the SELECT statements to include the required values in the selection for merging.

If you get undesirable results, study the merge reports to see why the merge process made the undesirable decisions. The merge report tells you what type of command caused the decision. Typically, the command that caused the problem is one of the following:

- A local OWNER/SUPGROUP command. The decision was exactly what you specified using a MERGERULE SOURCEID command. Alter the command to suit your needs.
- A local DATA/AUTHORITY command. The decision was caused by a MERGERULE SOURCEID command that applies to the profile. Alter the command as required.
- A global DATA/AUTHORITY command. The decision was caused by a MERGERULE DEFAULT command that applies as a fall-back to all profiles. You can alter the default to suit your needs; or add a MERGERULE SOURCEID for a specific group of profiles that need non-default handling.
- A built-in command. This command is a built-in fallback used in case of errors, conflicts, or lack of commands. MERGERULE commands have precedence over built-in rules; by specifying such a command, you can alter the decision to suit your needs.

How are access lists merged?

When a profile is present in both databases, merging the access list (ACL) is fairly straightforward. However, if a profile is present in only one of the databases, some preliminary work is required before merging the databases. If the merge is done without doing this work, some user IDs end up without access to a given resource because the resource is protected by a different profile after the merge.

If a profile is present only on the source database, merge processing searches for the *equivalent profile* in the current database. An equivalent profile is one that protects the same data sets or general resources as the source profile. When the merge is processed, the source file is created on the current system and added to the access list of the equivalent profile. In effect, the merge is adding a redundant profile to the current system. If a profile is present only on the current system, but it is affected by the merge, a similar process is used to add a redundant profile to the source system. No profiles are actually added to the source database. Merge just functions as though they were.

Table 271 shows examples of merge processing results for profiles that are only present in one of the databases being merged.

Table 271. Examples of merge processing for profiles that are not found in both databases

Source	Current	Action
`A.B.**` with ACL `X,Y,Z`	A.** with ACL W,X,Z	Profile A.B.** is added to the current database, with IDs W, X and Z on the access list.
`C.**` with ACL X,Y,Z	C.D.** with ACL W,X,Z	Profile C.D.** is added to the source database, with IDs X, Y and Z on the access list.

This process cannot always be followed. The other database does not always have an equivalent profile that protects all the relevant resources. In this situation, the profile is added as-is and the access list is processed based on the following guidelines.

Access list processing uses the `AUTHORITY` setting and checks it against user and group IDs to determine how to merge the access list entries. Entries are processed based on the following general rules:

- Access list entries that are only present on the source profile are copied as they are with the following exceptions:
  - Entries with a LOW authority are skipped.
  - Entries with a SOURCE or CURRENT authority where the profiles selected for merging do not include the user or group are skipped.
- All other access list entries are processed according to the following rules.
  - Entries with SOURCE authority use the source value.
  - Entries with CURRENT authority use the current value.
  - Entries with LOW authority use the lowest access level of the two assigned values.
  - Entries with HIGH authority use the highest access level of the two assigned values.

The process for evaluating and merging the access list entries depends on evaluating the AUTHORITY setting and checking user and group IDs.

Evaluating the AUTHORITY setting

Access lists and conditional access lists for data set and general resource profiles are merged according to the AUTHORITY setting applied to the profile.

- For data set profiles with a MERGERULE SOURCEID AUTHORITY setting for the high-level qualifier, the merge uses the specified AUTHORITY.
- For general resource profiles with a MERGERULE SOURCECLASS AUTHORITY setting for the class, merge uses the specified AUTHORITY setting.
- In all other cases, merge uses a MERGERULE GLOBAL AUTHORITY setting.

Roughly speaking, the meaning of the AUTHORITY setting can be interpreted as follows:

Table 272. AUTHORITY setting

Authority setting	Meaning
SOURCE	Implies that no applications from the source system fail after the merge.
CURRENT	Implies that all applications on the current system continue running after the merge.
HIGH	Implies that all applications continue to work after the merge.
LOW	Is a restrictive setting that only grants access if both databases agree on the level. In general, this setting requires you to determine which additional PERMITs are necessary after the merge. Then, you must add them manually.

Checking the user and group ID

For each source access list entry, the merge checks whether the ID is present on the current data base. This process takes MERGERULE SOURCEID RENAME commands into account and also handles the special IDs `*`, `&RACUID`, and `&RACGPID`.

If an ID is not present in the current data base, and is not merged, the access list entry is skipped. For all other cases, the access list entries are selected according to the rules listed in Table 273.

Table 273. Access list selection rules for merging profiles

Source vs Current	Authority	Action
source-only	SOURCE	Add entry to access list if ID selected
	CURRENT	Add entry to access list if ID selected
	HIGH	Add entry to access list
	LOW	Do not add entry to access list
source access < current access	SOURCE	Use source (lower) access
	CURRENT	Use current (higher) access
	HIGH	Use higher (current) access
	LOW	Use lower (source) access
source access = current access	*any*	Keep access list entry as it is
source access > current access	SOURCE	Use source (higher) access

Table 273. Access list selection rules for merging profiles (continued)

Source vs Current	Authority	Action
	CURRENT	Use current (lower) access
	HIGH	Use higher (source) access
	LOW	Use lower (current) access

Notes:

1. If an access list contains an undefined ID, warning message `CKR0679` is issued. If you see this message, clean up the database using VERIFY PERMIT before performing merge processing.
2. If a user or group is not selected to be merged but is already present in the current data base, an access list entry for that ID can be merged.

How are connects merged?

User group connections are not merged by using a SELECT statement. Instead, a MERGERULE CONNECT statement determines which user group connections are to be merged. When a connection is selected to be merged, MERGERULE DATA and MERGERULE AUTHORITY commands determine how. The following processing behavior determines how to process connections during merge processing:

- A user group connection can be merged if both the user and the group are present on the current system or are present after the merge.
- When a user group connection is checked to see if it must be merged, the merge checks the CONNECT setting. The setting is checked for the user, the group, and the default setting in that order. If no CONNECT setting is present for the user, or if the user is not selected, the group setting is checked. If no CONNECT setting is present for the group, or the group is not selected, the global setting is used.
- Finally, if a user is selected, the connection to the default-group is always copied if this default-group is available after the merge.

The following process describes how the merge decision is made in different situations:

1. If the user is selected and has a CONNECT setting, the connection is used as follows:

   NONE
   Connect not copied

   IFUSER, IFANY
   Connect copied

   IFGROUP, IFBOTH
   Connect copied if group is selected; else go on to step 2
2. If the group is selected and has a CONNECT setting, the setting is used as follows:

   NONE
   Connect not copied

   IFGROUP, IFANY
   Connect copied

   IFUSER, IFBOTH
   Connect copied if user is selected; else go on to step 3

3. If the selection includes the user, the group, or both, use the default CONNECT as follows:

   NONE
   Connect not copied

   IFANY
   Connect copied

   IFUSER
   Connect copied if user is selected

   IFGROUP
   Connect copied if group is selected

   IFBOTH
   Connect copied if both user and group are selected

After a user group connection has been selected to be merged, it must be decided how the connect is to be used. The decision is made based on a MERGERULE AUTHORITY command. Once again, the MERGERULE commands are checked for the user, the group, and the default, in that order. The merge decision is made based on the following processing rules:

1. If the user is selected, and a MERGERULE SOURCEID AUTHORITY is present for the user, that authority is used. Else, go on to step 2.
2. If the group is selected, and a MERGERULE SOURCEID AUTHORITY is present for the group, that authority is used. Else, go on to step 3.
3. If a MERGERULE DEFAULT AUTHORITY is present, that authority is used. Else, issue an error.

The authority found (`LOW`, `HIGH`, `SOURCE`, or `CURRENT`) is then applied to the connect-attributes.

How do I exclude a user or group?

If you do not want to merge a user or group, specify an `EXCLUDE` command for the user within the MERGE/ENDMERGE block. Alternatively, you can create a `SELECT` command that does not include the user or group. For example, the following example shows the code required to merge the entire data base except for the group *NOTTHIS*:

```
merge
 exclude class=group key=notthis
endmerge
```

The user or group ID might still show up in the commands generated in the following situations:

- The ID might occur in the `PERMIT` commands to add the user or group to access lists. This occurrence only happens if the ID exists in the current data base and the `AUTHORITY` setting is not `LOW`. To prevent this error, specify the AUTHORITY(LOW) attribute.
- The ID might be used for creating a user-group connection in CONNECT commands. This occurrence only happens if the following conditions are true:
  - The ID exists in the current data base
  - The other side of the user group connection is being merged with a `CONNECT` value other than `IFBOTH` or `NONE`.

  To prevent the IDs from showing up set the connect attribute to CONNECT(IFBOTH).

- The ID might be used as owner, default-group, etc. if it exists in the current data base; the merge process may then use it as a fall-back value. To avoid this, assign another ID as owner or superior group (using the MERGERULE SOURCEID OWNER and SUPGROUP commands), or change the DATA and AUTHORITY settings to alter the decisions made by the merge process.

How are general resource classes merged?

A general resource class is not merged if it is not defined in the Class Descriptor Table (CDT) of the current system. It is not merged because you cannot add profiles in a non-existing class to the RACF database.

A common use of merge is to combine databases at different release levels during an OS upgrade. If you have RACF databases on different release levels and intend to merge them, perform the merge on the higher level system. During merge processing, the generated commands are to add profiles in the newer general resource classes. For the merge process, use a database copy of the lower-level database instead of an unload version which uses the CDT of the lower-level system.

If a general resource class exists on the target system, but is inactive, profiles are merged normally. The merge process generates SETROPTS CLASSACT and SETROPTS GENERIC commands whenever necessary.

Chapter 10. RACF Access Monitor

The RACF Access Monitor function provides RACF administrators with the data required to remove unused or obsolete resource profiles and authorizations defined within profiles. RACF administrators and analysts can also use this function to test resource profiles and access rights by running simulations against a candidate RACF database. The candidate database can be one prepared using Security zSecure Admin RACF Offline, or a database on another z/OS system where you intend to host production processes.

Using the Access Monitor function, you can monitor access events and collect the data for reporting and analysis. From the reports, you can view and analyze the resource profile and access usage.

Note: Your installation must have the Access Monitor program for the z/OS system installed and configured before using the program. You must also have access to the data sets used to consolidate the access data. For details on the setup and configuration, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

The RACF database cleanup function consists of three components:

- The RACF Access Monitor program (C2PACMON) used for data collection.
- The CKRCARLA program that summarizes and saves the collected data so it can be analyzed.
- An ISPF menu component that allows you to specify selection criteria for reports, generate reports, analyze reports, and perform RACF database cleanup tasks.

The following processes provide the data to analyze access events and perform RACF database cleanup tasks.

Data collection

The RACF Access Monitor program (C2PACMON) collects the usage data on resource profiles and the authorizations defined within the profiles. To collect the required RACF information, the function dynamically defines several RACF exits to capture RACF events and collect the required information. When the Access Monitor program is running, it monitors access on a continuous basis.

The collected Access Monitor records are saved to disk at the end of each SMF interval. The SMF interval is specified by using the INTVAL parameter in member SMFPRMxx in PARMLIB. The default INTVAL parameter value is 30 minutes. The CKRCARLA program is used to combine the collected records and write them to a data set. Each type of access event is saved in a corresponding access record.

Data consolidation

Because access monitoring runs continuously, it collects a large amount of data. To maintain a manageable amount of data for reporting, the Access Monitor process summarizes the data collected at each interval on a daily basis. The summary removes redundant profile information and provides access counts on profiles with multiple access events. The summarized data is written to a daily consolidation data set. Daily consolidation data sets can be further consolidated on a weekly or monthly basis using the CKRCARLA procedures provided with

zSecure Admin. Administrators can also create custom consolidation jobs to consolidate access data sets for different time intervals. For example, an installation might want to consolidate three monthly data sets into a single data set to generate quarterly Access Summary or RACF Usage reports. These consolidation data sets are the data source for the Access Monitor reporting functions.

Report Generation

Users process the consolidated access data by running ad-hoc queries to evaluate the profile usage and access data. Processing can be set up and run interactively using the options available on the Access Monitor menu in the product.

The access data can also be processed using CKRCARLA. Two CARLa `NEWLIST` types are available for this purpose. The first, `ACCESS NEWLIST` uses the Access Monitor records to report about the collected RACF events. The second, `RACF_ACCESS NEWLIST` shows profiles in the RACF database and annotates these profiles with usage data from the Access Monitor records.

With proper record selection through the user interface or a CARLa program, Access Monitor reports can include the profiles of interest for a particular application. For example, you can report on all access permitted by the Global Access Checking table. You can also create commands to delete profiles that have not been used recently.

Figure 481 on page 645 provides an overview of the Access Monitor data collection, consolidation, and reporting process. In the following figure, user requests for access are captured using RACF exits. Access data is collected by the RACF Access Monitor (C2PACMON) and saved to a daily consolidation data set. The daily files can also be consolidated into weekly or monthly collections, for example. The consolidated data sets are the data source for the CKRCARLA program used to analyze and report on the access information. You can also use data from the RACF database as the data source for the reporting process. You can specify the same database used when the access data was collected or a candidate database. Depending on the options you selected, report output can be viewed from printed reports or ISPF panel displays. The reports are generated using the CKRCARLA program.

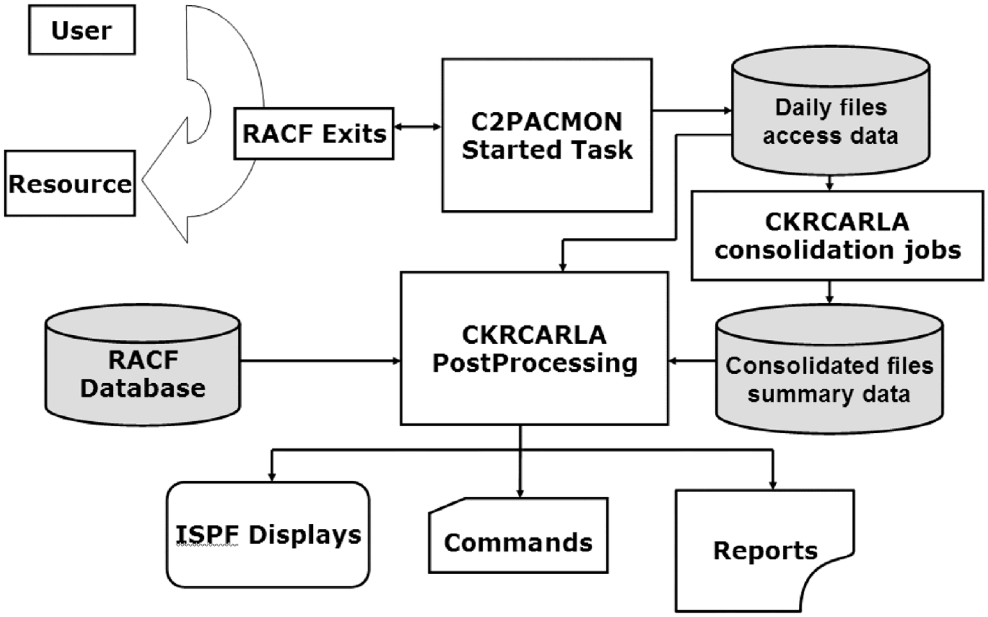


Figure 481. RACF Database Cleanup process program components and data flow

Collecting and consolidating data from the Access Monitor

The Access Monitor program runs as a started task. When the Access Monitor is running, it automatically collects access event data at a defined SMF interval (the default is 30 minutes) and writes event data to a data set. The SMF interval is defined by the INTVAL parameter in member SMFPRMxx in PARMLIB. The data collected for each event includes the following types of information:

- Resource name
- Profile name used
- Userid
- Jobname
- Port Of Entry (POE) information
- Access intent (READ, UPDATE, ALTER, and so on)
- Reason the access was granted
- Some attributes of the userid
- Date and time
- Number of events

Specifying Jobname and Port Of Entry collection

The Jobname and Port Of Entry information are present only if the Access Monitor task has been configured to collect that information. Collecting these fields makes consolidation less effective, so collect this information only insofar as you need it:

- The primary use of the JOBNAME field is with shared userids, such as those used in some JOB scheduling implementations, or those used for started tasks.
- The primary use of the UTOKEN_POECLASS field is with events, where access is granted using the conditional access list, such as for resources in the OPERCMDS class.

The person who sets up the Access Monitor task also configures the Access Monitor task to collect Jobname and Port Of Entry information. Discuss with this person for which userids or resource classes you need Jobname and Port Of Entry information.

Note: For instructions for installing and configuring the Access Monitor program and starting the task, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Daily collection and consolidation

At the end of the day, the collection data for each interval is consolidated into a daily data set. During the consolidation process, all records for similar events are combined and counted together. In the combined records, the date and time of the last occurrence for each event is kept. The date and time information about all previous occurrences is discarded. The summarized data is written to a consolidated daily Access Monitor data set, which is the data set most often used to generate reports.

The Access Monitor program automatically performs the daily consolidation process. Other consolidated Access Monitor data sets might be created depending on the procedures set up by the person who installed and deployed the Access Monitor. For example, the daily data sets might be consolidated into monthly data sets. Instructions for creating the consolidated Access Monitor data sets are provided in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. Users can also create their own Access Monitor data sets by consolidating existing data sets. See "Consolidating data collected by Access Monitor" on page 684.

Configuring Jobname and POE-data collection

If you require detail information about the jobname or the Port Of Entry (POE) for certain access monitor events, some configuration members must be changed to specify for which situations the information is collected. There are three configuration members involved. The person who does the installation and deployment can specify the data set name where these three members are located. By default, they are located in the general C2PACMON configuration data set, as specified in the C2PACPRM parameter.

- Collection of jobname information is controlled by the contents of the C2PAMJOB member. This member has a two column layout. An example is shown after this paragraph. The member name and the ruler line are not part of the member, but are shown here for clarity only. The ruler line highlights that the second column must start in position 10 of the record.

  ```
  C2PAMJOB
     ----+----1----+----2
     IBMUSER  YES
     C2PSUSER NO
  ```

  The first column contains a USERID for which jobname information is controlled. The second column can contain the value `YES` or any other value. Jobname information is collected only for those users for which the value `YES` has been specified. For users that are not included in the C2PAMJOB member, or that have any value other than `YES` specified, jobname information is not collected. Be sure that all information in this member is specified in uppercase.
- Collection of Port Of Entry information is controlled by the contents of the C2PAMRCL and C2PAMPCL members. These members each have a two column layout. Examples are shown after this paragraph. The member name and the

ruler line are not part of the member, but are shown here for clarity only. The ruler lines highlight that the second column must start in position 10 of the record.

```
C2PAMRCL
   ----+----1----+----2
   OPERCMDS YES
C2PAMPCL
   ----+----1----+----2
   CONSOLE  YES
   TERMINAL YES
```

The first column contains a resource class for which POE information is controlled. The second column can contain the value `YES` or any other value. The C2PAMRCL member specifies the resource class for which the access verification is done. This can be any RACF resource class, such as DATASET, FACILITY, or OPERCMDS. The C2PAMPCL member specifies the resource class (type) of the POE. The following POE classes are recognized: TERMINAL, CONSOLE, JESINPUT, APPCPORT, and SERVAUTH. POE information is collected only for those events for which the Resource class and the POE class both have the value `YES` specified. If either class specifies any other value, POE information is not collected for this Access Monitor event. Be sure that all information in these configuration members is specified in uppercase.

Updates to the three configuration members described here are effective for data collected after a restart of the C2PACMON started task or after the C2PACMON started task has done a consolidation run. For more information about restarting the C2PACMON started task, or the consolidation process as done by the C2PACMON started task, see the section about C2PACMON operator commands in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Setting up zSecure to analyze and report on Access Monitor data

The process to set up zSecure to analyze and report on access event information depends on what you want to accomplish. You can use this data for the following tasks.

- Review access data for a specific profile or set of profiles over a specific time period
- Analyze access data for RACF database cleanup (removing unused profiles and permissions)
- Prepare to move a production workload from one z/OS image to another z/OS image

The setup process for each task is the same. First, identify the data resources that provide the required access information. Then, use the Setup Input Files option (**SE.1**) to specify the selected data resources as the information source for the access event analysis and reporting processes.

Identifying data sources for the access information

Review access data from a specific time period

The Access Monitor consolidation data sets contain real-time access event information collected over varying time periods. Daily consolidation data sets provide information about the last access occurrence for each profile or profile group during a given day. Monthly consolidation data sets provide information about the last access occurrence for each profile or profile group during a given month.

To determine the first day a particular data set profile was used, choose a data source that includes the daily consolidation data sets for the time period you want to investigate. These data sets provide information about access events for each day within the time period covered by these data sets.

To determine whether a data set profile has been used within the last two months, use access data collected monthly as the data source. This information is available from monthly consolidation data sets. In this example, data set profiles that have not been used in the last two months are either absent from the access event data, or present with an old date and time information.

The person who configured the Access Monitor program can provide the names of the consolidation data sets for your site. You can also create customized consolidation data sets from the existing ones if you want to investigate a time period not covered by the existing data sets. For example, if you want annual data, you can consolidate the monthly consolidation data sets. See "Consolidating data collected by Access Monitor" on page 684.

Using the Access Monitor data to prepare for RACF database cleanup
RACF database cleanup allows you to remove unused profiles and permissions from the live RACF database. To get information about which resources to target for removal, designate the following data sets as Access Monitor data sources: the CKFREEZE data set and the RACF database from the same image where the Access Monitor records were created.

You can replace the (live or foreign) database by an UNLOAD data set to improve performance of the analysis and reporting functions. In most data centers, there is already an UNLOAD data set available that is refreshed daily. Ask your local administrator.

Using the Access Monitor data to prepare for moving a production workload from one z/OS image to another z/OS image
To use the Access Monitor information to prepare for moving a production workload from one z/OS image to another, designate the following Access Monitor data sources: the CKFREEZE data set and the RACF database from the image that is the candidate for running that production.

You can replace the (live or foreign) database by an UNLOAD data set to improve performance of the analysis and reporting functions. In most data centers, there is already an UNLOAD data set available that is refreshed daily. Ask your local administrator.

Defining the access information data sources

Use the Setup Input Files option (**SE.1**) to specify the data sets to use for analyzing and reporting on access event data.

You can add the required data sets to an existing input file set or create an input file set. An input file set is a collection of data sets or files to be used as a data source. The data set type for Access Monitor data sets is ACCESS. For details, see "SE.1 Setup - Input files" on page 1645.

After you have added the Access Monitor data sets and selected the input set, the data is available to zSecure. Use the Access Monitor menu options (**AM**) to generate reports, analyze access data, and perform RACF database cleanup tasks. For details, see the following sections.

- "Selecting and reporting using Access Monitor data sets" on page 649
- "Reporting on actual profile usage" on page 649
- "Comparing access results against another database" on page 656

- "Reporting on RACF Usage" on page 658
- "Performing RACF database cleanup tasks" on page 671
- "Consolidating data collected by Access Monitor" on page 684

Selecting and reporting using Access Monitor data sets

You can set up and generate Access Monitor reports from the Access Monitor menu. Figure 482 shows the menu which is displayed by entering the AM command in zSecure Admin.

```
   Menu         Options       Info    Commands     Setup
 ____________________________________________________________________________

                        zSecure Admin+Audit for RACF - Access
Option ===> ____________________________________________________________________

1      Access          Access summary by user or profile
2      Compare         Compare monitored access against current RACF database
3      Permit usage    Permit usage information for current RACF database
4      Connect usage   Connect usage information for current RACF database
5      Profile usage   Profile usage information for current RACF database
6      Member usage    Member usage information for current RACF database
7      Global usage    Global usage summary for current RACF database
8      Remove          Remove unused profiles and authorizations
9      Cleanup         Remove permits, dataset and general resource profiles
```

Figure 482. Access Monitor menu

Reporting on actual profile usage

The data collected by the RACF Access Monitor includes information about various aspects of the RACF access verification request and result processing. For example, the data includes information about the use of the Global Access Checking (GAC) table. The access data also provides detailed information about the use of discrete (data set) profiles. You can report on this data interactively using the **Access summary by user or profile** option (**AM.1**) available on the zSecure Admin main menu.

Note: You can also create reports using the `NEWLIST TYPE=ACCESS` statement in a batch job. For details, see "ACCESS: Access Monitor Records" on page 953.

Setting up the report

The Access Summary report is based on input collected by the Access Monitor program. The report uses the ACCESS data sets specified in SETUP FILES. This report does not include information from the specified RACF input source. It only shows the actual profile and access usage as recorded by the Access Monitor program. It does not show access groups or data for profiles that were not used during the access monitor data collection period.

To begin reporting on RACF access request activity for `userid`s or resource profiles, select option **AM.1** from the zSecure Admin main menu. This option opens the selection panel shown in Figure 483 on page 650.

```
                        zSecure Suite - Access - Access
Command ===> ____________________________________________________________

Show records that fit all of the following criteria:
Userid  . . . . . . . . ________  (userid or EGN mask)
Complex . . . . . . . . ________  (complex or EGN mask)
SAF resource class  . . ________  (class or EGN mask)
SAF resource name . . . ____________________________________________
RACF match on . . . . . ____________________________________________

Advanced selection criteria
_  Further selection                    _ Date selection

Output/run options
1  1. Summarize by userid      2. Summarize by member class and profile
 _  Show configured fields
 _  Print format          Customize title     Send as email
       Background run     Full page form
```

Figure 483. RACF Access Monitor - Selection panel to generate Access Summary report

Use this panel to specify the report selection criteria and the report output and run options. Report results are output to the ISPF display by default. If you want the results to be printed or sent using email, select the **Print format** option.

On the report selection panel, if you leave the selection criteria blank and press **Enter**, all Access Monitor event records are displayed.

For field help, position your cursor in the field, then press **F1**. For panel help, press **F1** from the command line.

Figure 483 shows the selection panel to set up the Access Summary report. Use this panel to specify the selection criteria and the output and run options to generate the report.

Specify selection criteria

Many access monitor records contain information about both the resource name specified by the application and the profile name used by RACF. Use the report selection criteria to specify the application resource name in the **SAF resource name** field and the RACF profile name in the **RACF match on** field. You can use regular pattern matching on both fields.

For the **RACF match on** value, you can specify a RACF profile name. The profile can be an individual profile or a member in a grouping-class profile.

Selecting on either field can be useful because the profile name might be absent from the access event data under some circumstances. For example, when data set access is permitted through the Global Access Checking (GAC) table, RACF does not use a real data set profile. Consequently, the profile field is empty but the resource name is present. In contrast, in the access monitor records for define/delete events, the resource name might be absent. For example, the resource name is absent for RACF commands where the user directly specifies a RACF profile and a resource name is not used.

Specify advanced selection criteria

Use the **Advanced selection criteria** to further narrow the selection criteria. If you choose one of these options, you are prompted to specify the criteria when you press **Enter** on the report selection panel. Figure 484 on page 651 shows the selection criteria available for the Further selection option.

```
                    zSecure Suite - Access - Further selection
 Command ===> ____________________________________________________________
 All access monitor records
 Specify further selection criteria:
Jobname . . . . . . . . . _____________________________(jobname or EGN mask)
Port Of Entry class . . . _____________________________ (class or EGN mask)
Port Of Entry . . . . . . _____________________________(POE or EGN mask)

Select access records(Y/N/blank)
 _  Use of commands to add/delete dataset and general resource profiles
 _  Use of global access checking table
 _  Use of discrete profiles               _  Access attempts undefined users
 _  System special authority used          _  User has special attribute
 _  Operations authority used              _  User has operations attribute
 _  Installation exit used

 Action against resource  Intended access          Result
 _   Define              _ __ 1. Read             _ Success
 _   Delete                   2. Update           _ No profile
 _   Addvol                   3. Control          _ Not authorized
 _   Chgvol                   4. Alter            _ Other
```

Figure 484. Access Summary report - Further selection criteria

If the option **Show configured fields** has been selected on Figure 483 on page 650, the top block of Figure 484 allows selection of fields: Jobname, Port of Entry class, and Port of Entry. These fields cannot be selected, and are reported as empty, unless C2PACMON has been configured to collect this information.

The two other parts of this selection panel are always available and allow selection of characteristics of the profile and the event or the user at the time of the event. For field descriptions, press F1 for help.

The **Use of global access checking table** option provides an overview of the actual usage of the global access checking (GAC) table. This report provides information that is difficult to obtain in any other way. The GAC report results show all access that was permitted because the resource matched a profile name in the global access checking table. In the Access Summary report, the information shown is centered around the resources that were accessed. The report does not include information about the actual GAC Table entries used - just that a GAC Table entry was used to grant access. In contrast, the Global Usage option **AM.7** provides a report on the use of the GAC Table. The AM.7 report is centered around the GAC Table and does not provide information about the actual resource or users that were permitted access.

If the Access Monitor data is collected on a z/OS V1.13 system or a z/OS system with PTFs UA61826 and UA61827 applied, the Access Monitor records include information about the authority used to allow access. The record also contains information from the ACEE about the current system level SPECIAL and OPERATIONS attributes of the user. Selection on the value N is only available if a CKFREEZE data set for the applicable system is allocated and if the CKFREEZE data set indicates that the required support is installed.

In the last selection block of Figure 484, you can specify selection criteria based on the following options.

- Use **Actions against a resource** criteria to select records based on the action taken during the event. For example, if you select Delete, the Access Summary report includes access records with information about delete profile actions.
- Use **Intended access** criteria to select records based on access level and an operator. For example, to include information about all access events where the

user requested Update access or higher, enter the > operator in the first field and 1 (Read access) for the Access level in the second field. To include information about access events where the user requested Read access, specify the = operator.

- Use the **Result** criteria to select records based on the outcome of an access event.

Figure 485 shows the advanced selection criteria available for the Date selection option which allows you to select records for a particular period.

```
                        zSecure Suite - Access - Date selection
Command ===>

Date selection
From date . . . . ________    Until date  . . . ________

Valid date formats are "01JAN2009", "2009-12-31", TODAY, or TODAY-nnn.
Specific dates entered on this panel are meaningful only if represented in the
set of Access Monitor input data sets. For additional information see HELP.
```

Figure 485. Access Summary report - Date selection criteria

Generate report output

The report output is organized based on the option selected in the **Summarize by** field.

- The **1. Userid** option generates a report in which the results are organized by `userid`. On reports shown on the screen, use the **S** command on any userid event entry to view more detailed information about the resource class and name. In a printed report, the resource class and resource name are shown at a secondary level.
- The **2. Member class and profile** option generates a report with the results organized by resource class and resource name with a secondary level for the `userid` information.

  The option name **Member class and profile** is used to emphasize that this value represents the resource class as used by the application.

If **Show configured fields** is selected, fields Jobname, POE, and POE class are available on the **Further selection** panel and are included in the generated reports. These fields are empty, unless C2PACMON has been configured to collect this information.

Summary results are shown on the ISPF screen by default. To generate a printed report, select the Print format options. For details on the Print option settings, press F1 for help.

Interpret the results

The information available in the access monitor event records is always shown in a summary format. This approach reflects the fact that the Access Monitor data sets used as a data source are always already a summary of multiple events. As mentioned in “Collecting and consolidating data from the Access Monitor” on page 645, the daily collection data sets provide a sequence of half-hour summaries of access event data. The daily consolidation data sets provide a single summary of 24 hours of access event data.

Figure 486 on page 653 shows an example of the Access Summary report results summarized by Userid.

```
IBM zSecure ACCESS summary                                    Line 1 of 8
Command ===> _____________________________________________ Scroll===> PAGE
Access monitor records for Userids like *       27 Jun 2009 17:03
   Occurrence Userid   Name                 First occurrenc Last occurrence
__         30 BCCG011                      13Mar2009 11:29 13Mar2009 11:29
__         54 C2PSUSER RECVS EMAIL VIA NJE  13Mar2009 11:25 13Mar2009 11:30
__          8 C2XTST1  C2PACMON TEST USER1  13Mar2009 11:29 13Mar2009 11:29
__          8 C2XTST2  C2PACMON TEST USER2  13Mar2009 11:29 13Mar2009 11:29
__          8 C2XTST3  C2PACMON TEST USER3  13Mar2009 11:29 13Mar2009 11:29
__         40 RACFAS   USER FOR RACF AS     13Mar2009 11:29 13Mar2009 11:29
__        358 RCCSL01  JOHN SMEDLINE SPEC.  13Mar2009 11:27 13Mar2009 11:30
__         62 STRTASK  DIV STARTED TASK USR 13Mar2009 11:28 13Mar2009 11:30
****************************** Bottom of Data ********************************
```

Figure 486. Access summary report - Event overview by userid

Reviewing high-level access event information: Both the Access Summary report formats (**userid** and **member class and profile**) provide the same detail information. Only the hierarchy and the access counts shown on the intermediate summary levels are different. This example focuses on two types of information shown in reports. The number of times an access event occurred and the date and time of the first and last occurrence.

Occurrence fields

This number reports the total number of times that the events on this line occurred. For example, the entry for the `userid RCCSL01` in Figure 486 reports that this userid was used for 358 events.

```
__        358 RCCSL01  JOHN SMEDLINE SPEC.  13Mar2009 11:27 13Mar2009 11:30
```

To see more detail on these events, type **S** in the field for the entry to open the detail panel shown in Figure 487.

```
 IBM Security zSecure ACCESS summary                                Line 1 of 7
Command ===> _____________________________________________ Scroll===> PAGE
 Access monitor records for Userids like *       27 Jun 2009 17:03
   Occurrence Userid   Name                 First occurrenc Last occurrence
          358 RCCSL01  JOHN SMEDLINE SPEC.  13Mar2009 11:27 13Mar2009 11:30
   Occurrence Intent   Type   AccRC
__        228 READ     Auth       0
__         10 READ     Auth       4
__         22 UPDATE   Auth       0
__          4 UPDATE   Auth       8
__         86 ALTER    Auth       0
__          2 ALTER    Auth       8
__          6 DEFCREAT Define     0
****************************** Bottom of Data ********************************
```

Figure 487. Access summary report - Event overview by Access Intent

From the panel shown in Figure 487, the report shows 22 of the events are related to an UPDATE request. Selecting the UPDATE entry, opens another detail panel showing the resource names used during the UPDATE events.

```
  IBM Security zSecure ACCESS summary                                Line 1 of 4
Command ===> ____________________________________________________ Scroll===> PAGE
All access monitor records                      28 Jun 2009 01:48
   Occurrence Userid   Name                 First occurrenc Last occurrence
          358 RCCSL01  JOHN SMEDLINE SPEC.  13Mar2009 11:27 13Mar2009 11:30
   Occurrence Intent   Type   AccRC
           22 UPDATE   Auth       0
   Occurrence Class
           10 DATASET
   Occurrence Resource
__          2 CRMBE01.C2PACMON.T#TIM.IOCONFIG
__          2 CRMBE01.C2PACMON.T#TIM.UNLOAD
__          4 CRMBE01.RCCSL01.SPFTEMP0.CNTL
__          2 C2PACMON.EZOS.DATA.D090313.T1221.C2PACMON
****************************** Bottom of Data ********************************
```

Figure 488. Access summary report - Event overview by resource class (profile)

You can then use the **S** command again to view details about the DATASET class resources. For example, selecting one of the DATASET class entries opens a panel where you can see additional information about the event such as the Profile key as shown in Figure 489.

First occurrence, Last occurrence fields

These fields report the first time the access event occurred and the last time the access event occurred in a given time period. The values in these fields depend on the type of consolidation data set used as data sources for the reports. The first occurrence shows the earliest date present in the data sources for the access time. As the section "Collecting and consolidating data from the Access Monitor" on page 645 explains, the meaning of the date value depends on the level of consolidation applied to the ACCESS data sets used as data sources. The First occurrence column indicates an approximate first use and has the precision of the consolidation period. If you are using consolidated weekly Access Monitor data sets, the **First occurrence** can only show the first week that access occurred.

Reviewing detailed event information: From the overview panels in the Access summary report, issue an **S** line command for any entry to view more detailed information about a particular event type. Figure 489 shows more information about the UPDATE requests from `userid` RCCSL01 including the resource class, resource name, and profile key used.

```
IBM Security zSecure ACCESS summary
Command ===> ____________________________________________________
Access monitor records for Userids like *
   Occurrence Userid   Name                 First occurrenc Last occurrence
          358 RCCSL01  JOHN SMEDLINE SPEC.  13Mar2009 11:27 13Mar2009 11:30
   Occurrence Intent   Type   AccRC
           22 UPDATE   Auth       0
   Occurrence Class
           10 DATASET
   Occurrence Resource
            2 CRMBE01.C2PACMON.T#TIM.IOCONFIG
   Occurrence Profile key used
            2 CRMBE01.*.*.**
   Occurrence Complex  Syst RGPCAVP GUGSOPGX SO   First occurrenc Last occurrence
            2 SYS1     EZOS         G             13Mar2009 11:30 13Mar2009 11:30
   Occurrence Timestamp
__          1 13Mar2009 11:30
  ****************************** Bottom of Data ********************************
```

Figure 489. Access summary report - Event overview by resource (member) name

This panel shows the `userid` RCCSL01 issued 22 requests to UPDATE a resource over the given time period. In this example, the time period is one day. To compare this information against the current profile and access list definitions in the current RACF database, use option **AM.2**. A comparison can be useful to determine how a particular userid or resource has been affected by changes to the RACF database.

You can also use this panel to get detailed event information such as the access intent, the event result, and the resources used. For example, from the information shown in Figure 489 on page 654 you can gather the following information.

1. Userid `RCCSL01` issued 22 request to UPDATE a resource.
2. The request was permitted (return code, **AccRC**=`0`).
3. The UPDATE requests were for data set resources.
4. The resource that was updated was CRMBE01.C2PACMON.T#TIM.IOCONFIG, which was satisfied using profile CRMBE01.*.*.** .
5. This same event occurred twice during the measurement period, one quickly following the other on March 13th 2009.

This panel also shows the request and access flags in effect for **RGPCAVP** , **GUGSOPGX**, and **SO**. Table 274, Table 275, and Table 276 provide flag field descriptions.

Table 274. Access Summary report - RGPCAVP flag fields

Flag	Description
R	The RACF Indicator is on (Y) or off (N) or not specified (blank).
G	A generic profile is requested.
P	Return of a Private/CSA profile is requested.
C	This request is part of RACF command processing.
A	The DEFINE request performs an internal authorization check.
V	The DEFINE request only verifies authorization.
P	This request is the result of automatic propagation.

Table 275. Access Summary report - GUGSOPGX flag fields

Flag	Description
G	A generic profile is requested.
U	The requesting `userid` is not RACF defined.
G	An entry in the global access checking table was used.
S	System special authority used.
O	Operations authority used.
P	The requesting task is Privileged or Trusted.
G	Access requested for GROUP.
X	Installation exit used.

Table 276. Access Summary report - SO flag fields

Flag	Description
S	User's ACEE had the system-wide SPECIAL bit set at the time of the check.

Table 276. Access Summary report - SO flag fields (continued)

Flag	Description
O	User's ACEE had the system-wide OPERATIONS bit set at the time of the check.

Selecting the **Occurrence Timestamps** entries opens the access event record detail display as shown in Figure 490.

```
IBM Security zSecure ACCESS summary
Command ===> ____________________________________________________
All access monitor records


  Access summary
  Security complex name         SYS1
_ RACF userid                   RCCSL01  JOHN SMEDLINE SPEC.
  Access intent                 UPDATE
  Record type                   Auth
_ System name                   EZOS
  SAF resource class            DATASET
_ SAF resource name             CRMBE01.C2PACMON.T#TIM.IOCONFIG
  Timestamp of last occurrence  13Mar2009 11:30
  Access count                  1

  Request flags                           Define flags
  RACFIND                       No        Command
  Limit to generics             No        Use internal RACROUTE AUTH
  Private/CSA (no global)       No        Verify
                                          Propagated
  Access time effect
  RACF profile key used         **
  RACF Profile type used        GENERIC
  Access allowed                READ
  RACF return code              0

 Access flags (common)                   Access flags (rare)
 Obtained generic              Yes       Privileged/trusted user       No
 Undefined user                 No       Group used                    No
 Global access table used       No       Installation exit used
 Special authority used
 Operations authority used

 Access-time user attributes
 User systemwide SPECIAL
 User systemwide OPERATIONS
```

Figure 490. Access summary report - Access Event record detail display

Comparing access results against another database

Using one of the advanced options of the Access monitor data analysis, you can also compare historical data against a current RACF database. This function is available from option **AM.2** in zSecure Admin. The current RACF database is the one that you have specified in SETUP, by default it is the current system RACF database.

Comparing the actual usage data against the RACF database can help verify that proposed changes to the RACF database do not negatively affect the production environment. For example, if a profile identified for removal was recently used to grant access to a resource, you can communicate with the users or groups that use the resource about the proposed change before putting it into production. You might also run a comparison to understand the effects of changing the RACF database in use or moving an application to another system.

If you prefer to run an Access monitor function using a batch job, use the NEWLIST TYPE=ACCESS statement with the SIM_* fields to perform a compare. Option AM.2 provides the following selection fields:

```
  Menu         Options       Info    Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - Access - Compare
 Command ===> ____________________________________________________________

 Show records that fit all of the following criteria:
 Userid  . . . . . . . . ________  (userid or EGN mask)
 Complex . . . . . . . . ________  (complex or EGN mask)
 SAF resource class  . . ________  (class or EGN mask)
 SAF resource name . . . ________________________________________________
 RACF match on . . . . . ________________________________________________
 Comparison selection
 Simulated results . . . /  Same      /  Less       /  More
 Profile used  . . . . . 3  1. Same   2. Different  3. All

 Advanced selection criteria
 _  Further selection                  _  Date selection

 Output/run options
 1  1. Summarize by userid      2. Summarize by member class and profile
 _  Show configured fields
 _  Print format          Customize title     Send as email
       Background run     Full page form
```

Figure 491. RACF Access Monitor - Access - Compare selection panel

The selection panel for option AM.2 provides many of the same selection criteria available for option AM.1. The additional selection options available are based on the **results** of comparing actual successful access events to access events that would be permitted using the selected RACF data source. The selected RACF data source is the one specified using the Setup Files option (SE.1). You can compare access based on the access result or based on the profile used for allowing or preventing access. The resulting reports all have a similar layout. Figure 492 shows an example of the report.

```
  Menu         Options       Info    Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - Access - Compare
 Command ===> ____________________________________________________________

 All access monitor records
    Occurrence Userid   Name                 First occurrenc Last occurrence
    __     1961 BCCG011  JOHN SMEDLINE          1Apr2009 08:14 30Apr2009 19:23
    Occurrence Intent   Type   AccRC SimRC
    __      686 READ     Auth       0     4
    __      934 READ     Auth       0     8
    __        1 READ     Auth       4     8
    __        2 CONTROL  Auth       0     8
    __        1 DEFDELET Define     0     8
    __        7 DEFDELET Define     0     4
    __        9 ALTER    Auth       0     4
    __       18 ALTER    Auth       0     8
    __      196 ALTER    Auth       0     4
    __       22 ALTER    Auth       4     8
    __       77 ALTER    Auth       4     8
    __        8 DEFCREAT Define     0     4
```

Figure 492. RACF Access Monitor - ACCESS summary simulated access is less report

In Figure 492 on page 657, the **AccRC** column shows the access that was historically permitted. The **SimRC** column shows the access that would be permitted using the current RACF data source. These differences might be caused by any of the following events:

- profile added or removed
- access list changed
- universal access changed
- warning mode changed
- use of operations or group-operations
- access through the special attribute

You can analyze the differences and check if these results are expected based on your selected RACF data source. Using the general selection criteria and the **summarize by** selection option, you can focus on the users or the resources that are important in your environment.

Reporting on RACF Usage

The Access Monitor data sets contain information collected by monitoring actual access attempts on the system. However, these data sets do not contain information about the resource profile definitions themselves. Also, the Access Monitor data sets cannot provide any information about profiles or access list entries that were not used. To report on all profiles and their information, you need data from the RACF database. Use Access monitor options AM.3 through AM.7 to generate reports that integrate information from the defined profiles in the RACF database with information about actual usage from the Access Monitor data sets.

Counting access events

To report on the use of all profiles and entries in the selected RACF data source, the usage information in the Access Monitor data sets needs to be matched to the correct profiles, Access List (ACL) entries and group connections. This matching process is not always straightforward. For example, in the RACF database, a data set profile for ABCD.** has an ACL with two groups and a single userid. The definition of the profile is:

```
DATASET Profile and ACL User profile

ABCD.**                 USER1
UACC    NONE             NAME     TEST USER1
USER1   READ             DFLTGRP  SYS1
GRP1    UPDATECONNECT    SYS1
GRP2    UPDATE
```

In this example, the request of USER1 to read data set ABCD.TEST is easily matched against profile ABCD.**, and it is easy to determine that the access list (ACL) entry used is the one for USER1 because this userid has specific READ access to the ACL. However, matching and counting access attempts is not always that easy. Consider another set of definitions like the previous example:

```
USER2
NAME        TEST USER2
DFLTGRP     SYS1
CONNECT     SYS1, GRP1, GRP2
```

If USER2 also tries to read data set ABCD.TEST, the ABCD.** profile clearly matches. However, how can you determine which ACL entry should be used? The USER2 ID is connected to two groups and both groups allow access.

zSecure Admin matches the access request for USER2 against both ACL entries. If there were a specific ACL entry for USER2, the access would be matched against that specific entry instead of the group entry. Just like RACF, zSecure Admin always uses the most specific entry for matching. In this case USER2 is not covered by a specific ACL entry. Consequently, for this access request zSecure Admin counts USER2 as having two matching entries: one because of membership in GRP1 and the other because of membership in GRP2.

zSecure Admin has a similar process to mark that a particular group-membership is used. For the first access request by `USER1`, no group-membership was used, so its group connection is not marked as used. For the second situation for `USER2`, both the group-connections to GRP1 and the GRP2 are marked as been used.

The matching of profiles to resource access requests becomes even more complicated for grouping resource classes. In the following example, you can get some idea of the complexity by looking at some CICS transaction profiles. Grouping class profiles RESGRP1 and RESGRP2 definitions both have as member the transaction CEMT with an ACL that contains USER1.

```
GCICSTRN RESGRP1       GCICSTRN RESGRP2
Member   CEMT          Member    CEMT
ACL      USER1  READ   ACL       USER1   READ
```

When CICS is started, the relevant resource classes are RACLISTed which loads all the relevant profiles into a dataspace and merges the grouping resource class profiles.

When USER1 runs the transaction CEMT two resource profiles grant access to USER1. Again, zSecure Admin matches the access against both profiles and both ACL entries. The result is that both profiles and both ACL entries are marked as used. Actual situations might be more complex. For example, you might have multiple profiles with different access lists that have both users and groups on the access list. Some situations might be more simple. For example, you might have two or more grouping profiles that do not cover any member resources.

The matching is done during the post-processing phase using the specified RACF data source. This information about groups, ACLs, and grouping resource profiles is not present in the Access Monitor data sets, but is the result of a simulation process. It can easily be repeated using the same Access Monitor data sets, but for a different RACF input source. The results of the matching and counting of access monitor events against the RACF profiles and information can be generated using the `RACF_ACCESS NEWLIST` that you implicitly use when you run one of the options **AM.3** to **AM.8**, available from the zSecure Admin main menu.

Creating RACF Usage reports using data from Access monitor and the RACF database

Use the RACF options (**AM.3 -AM.7**) to relate the ACL (permit), connect, and profile definitions in the current RACF database to the actual resource access events and profile usage recorded in the Access Monitor data sets. (shown in Figure 493 on page 660). This information can help you understand the impact of changing RACF database profiles and ACLs before moving the changes to production. You can also use the data to identify and investigate unused or obsolete profiles and authorizations.

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                        zSecure Admin+Access for RACF - Access
Option ===> ____________________________________________________________________

1      Access          Access summary by user or profile
2      Compare         Compare monitored access against current RACF database
3      Permit usage    Permit usage information for current RACF database
4      Connect usage   Connect usage information for current RACF database
5      Profile usage   Profile usage information for current RACF database
6      Member usage    Member usage information for current RACF database
7      Global usage    Global usage summary for current RACF database
8      Remove          Remove unused profiles and authorizations
9      Cleanup         Remove permits, dataset and general resource profiles
```

Figure 493. Access Monitor menu

You can specify the type of data source for the RACF Usage reports. The following options are available:

1. If you use data sources from both the RACF database and the Access Monitor program, the report provides information about actual use of both permits and connects.
2. If you only use the RACF database as a data source in combination with the SIMULATE RACF_ACCESS option, the report provides information about the permits and connects permitted based on the RACF database profile definitions. The output is an exploded view of all permits and connects defined in the RACF database, including the effects of RACLIST merge processing.

The information from the RACF data source is combined with the data from the Access Monitor data sets. The resulting report provides information about use of the profiles and information in these profiles. For example, a Permit Usage report can show that the access list for a resource profile in the RACF database allows UPDATE access to 10 different groups. But the Access monitor event data for the last six months shows that only one group has requested READ access to the resource.

Each record shown in the RACF Usage reports represents a single access list (ACL) entry. The reports also include special pseudo entries for the UACC and the high-level qualifier <HLQ> of the resource. Using separate records for each ACL entry makes it easy to process the information and present detail information about how often a particular ACL entry was involved in allowing or preventing access to the resource.

The process to set up the reports and analyze the information in the RACF usage reports is similar for all the Access monitor reports. This documentation illustrates the process using the RACF Permit Usage report. You can follow the same process for the other reports.

For more information about the RACF Access Usage reports including detailed field descriptions, see “RACF_ACCESS: Connects and permits” on page 1213.

Setting up and generating the reports

This procedure illustrates how to set up and generate the Permit usage report. You can use this same process to generate the other Access monitor reports. However, the entry fields and selection criteria are not the same for each report type.

The Permit usage report shows profiles and their ACL entries as defined in the RACF database combined with the relevant usage data from the Access Monitor

data sets. To begin reporting permit usage, select option **AM.3** from the zSecure Admin main menu to open the selection panel shown in the Figure 494.

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
              zSecure Admin+Audit for RACF - Access - Permit usage
Command ===> ____________________________________________________________

Show permits that fit all of the following criteria:
Permit id . . . . . . . ________  (permit id or EGN mask on access list)
Class . . . . . . . . . ________  (class or EGN mask)
RACF profile name . . . ________________________________________
Complex . . . . . . . . ________  (complex or EGN mask)
Show accesses . . . . . _  Non-zero counts     _  Zero counts

Profile to use  _  1. Use historic profile name in access summary if present
                   2. Simulate access in database to find current profile

Advanced selection criteria
_  Further selection                    _  Date selection

Output/run options
_  Print format          Customize title     Send as email
      Background run     Full page form
```

Figure 494. Access - Permit usage report

Use this panel to specify the report selection criteria and the report output and run options. Report results are output to the ISPF display by default. If you want the results to be printed or sent using email, select the Print format option.

To view all the profiles and ACL entries, leave the selection criteria blank. Then, press **Enter**.

For detailed field information about any panel, position your cursor in a field and press F1 to view the help. For panel help, position your cursor on the command line, then press F1.

Specify selection criteria:

Show permits that fit all the following criteria:
In these selection fields, you can use special values such as `-UACC-` and `-other-` as well as patterns to match the values for other selection criteria fields.

Show accesses
For this selection criteria, type an option number to base the record selection on ACL entries that are used (**non-zero counts**) or ones that are not used (**zero counts**).

Profile to use

Use this criteria to indicate whether reporting is based on profiles present in the Access Monitor data sets, or on the profiles as currently defined in the RACF data source.

1. The **1. Use historic profile name in access summary if present** option bases reporting on the profile used at the time of access checking. This profile is found in the Access Monitor data sets. Access requests that refer to a profile that still exists are counted in the typical way. Access requests that refer to an existing profile are counted in the normal way.

If that profile no longer exists, zSecure Admin does not match the access request to any real profile, but instead the access request is counted on dummy profile `<hlq>.**` for ACL entry `-other-`.

2. The **2. Simulate access in database to find current profile** option discards the profile recorded at the time of the access request. The resource name is used to locate the currently applicable resource profile. This operation is like a replay of the historic events against the current database.

Both these reporting options have their advantages. For example, if you are looking at the data from a usage perspective for data base cleanup purposes, select option 1, **1. Use historic profile name in access summary if present**. If you are evaluating the effectiveness of your current definitions, select option 2, **2. Simulate access in database to find current profile**. There is not much difference in the report output for these two options if no significant changes were made in the current RACF database since the time the access event data was recorded.

Specify advanced selection criteria: Use the **Advanced selection criteria** to further narrow the selection criteria. After selecting one of these options on the report selection panel, press enter to specify information for the selected criteria.

Use the **Further selection** option to specify criteria based on access request results, the profile or connect creation date, and the access level used in the access request. Figure 495 shows the selection criteria available for the Further selection option.

```
 Menu         Options       Info    Commands     Setup
_____________________________________________________________________________

               zSecure Admin+Audit for RACF - Access - Further selection
Command ===> _____________________________________________________________

Access selection
#Accesses allowed . . . __  _________
#Accesses prevented . . __  _____
#Accesses unexplained    __  _____

Permit selection
Creation date from  . . _________  Until   _________

_  Highest access used less than access allowed

Access allowed           Highest access used   Lowest violation
>=  _  1. Read           <=  _  1. Read        >=  _  1. Read
       2. Update                2. Update             2. Update
       3. Control               3. Control            3. Control
       4. Alter                 4. Alter              4. Alter
```

Figure 495. RACF Usage report - Further selection criteria

Selecting records based on Access request result

This option selects records based on the outcome of the access requests.

access allowed
The ACL entry grants access at the requested level and the Access Monitor data sets also recorded a successful access.

access prevented
The ACL entry denies access at the requested level, and the Access Monitor data sets also recorded a failed access.

unexplained
Category for all other access results. For example, events in the unexplained category include attempts where access should have been permitted based

on the ACL entry show up as failed attempts in Access Monitor data sets, or vice versa. The most common reasons for an access record to be included in the unexplained count are changes in the ACL, UACC, or (group-)operations attribute.

Each of these options requires two data points: The first field specifies an operator, the second field specifies a target number of occurrences. For example, use the `Access allowed` option to investigate successful access attempts. To find access events in which access was successfully permitted more than 100 times, type `>` in the first field and `100` in the second field.

Selecting records based on profile creation date

On the Further Selection panel for the Permit and Profile Usage reports, use the **creation date** option to select records based on the profile creation date. Unfortunately, you cannot select on ACL creation date because RACF does not record when an individual ACL entry was added or changed.

On the Further Selection panel for the Connect Usage report, the date selection criteria selects access event records based on the date the user was connected to the group.

Example

To avoid reporting permit usage for new profiles, you can specify an **Until** date of `today-nnn` to suppress all recently created resource profiles.

Selecting Access level usage

Use the access levels options to select records based on **Access allowed**, **Highest access used** and **Lowest violation created**. The lowest violation option selects records with the minimum access level that resulted in an access violation.

Each of these selection options requires an operator value and an access level setting. The operator field sets a threshold for selecting records based on access levels and outcomes. For example, in the first entry field for the **Access allowed** option, typing **1** in combination with the default operator selects all records with successful access attempts using READ access or higher.

For a list of operators, press F1 on the field to see the help.

Example

If your organization has a policy of allowing access to resources at the minimum level required, you can identify resource profiles with access levels higher than the minimum by specifying the **Access allowed** selection criteria in combination with the **Highest access used** option. The accesses shown in the resulting report can be used as target for a *use it or lose it* cleanup approach. To avoid populating the report with access events where users request access to their own resources such as user-dataset profiles, specify `<=alter` for the **Access allowed** criteria.

Selecting the advanced selection criteria **Date selection** option opens the panel shown in Figure 496 on page 664. Use this panel to specify record selection criteria for a particular period.

```
                        zSecure Suite - Access - Date selection
Command ===>

Date selection
From date . . . . ________    Until date  . . . ________

Valid date formats are "01JAN2009", "2009-12-31", TODAY, or TODAY-nnn.
Specific dates entered on this panel are meaningful only if represented in the
set of Access Monitor input data sets. For additional information see HELP.
```

Figure 496. Access Summary report - Date selection criteria

Specify report output options: Report results are output to the ISPF display by default. To print or email the report, select the **Print format** option and specify the options you want to use. Press F1 in any field to get help.

Reviewing report results

Figure 497 provides an example from the Member Usage report showing the first level results for all CICS-related resource classes.

```
RACLIST merged profile permits and UACC
Command ===> ____________________________________________
Permits by member, Member classes like %CICS*
   Allowed Deny  Unexp LastUse MemClass Complex
__       0     0     0         ACICSPCT SYS1
__       2     0     0 6Apr09  CCICSCMD SYS1
__       0     0     0         DCICSDCT SYS1
__       0     0     0         MCICSPPT SYS1
__      81     0     0 10Apr09 TCICSTRN SYS1
*************************** Bottom of Data ********************
```

Figure 497. RACLIST merged profile permits and UACC report

The report view shown in Figure 498 on page 665 only shows the resource classes as used by CICS to check access. These resources are all member classes. To view details for a member class, type **S** in the entry field. Then, press enter to open the detail view. Figure 498 on page 665 shows the detail view for the TCICSTRN member class.

```
RACLIST merged profile permits and UACC
Command ===> ____________________________________________________
Permits by member, Member classes like %CICS*
   Allowed Deny  Unexp LastUse MemClass Complex
   Allowed Deny  Unexp LastUse MemClass Complex
__         81     0     0 10Apr09 TCICSTRN SYS1
   Allowed Deny  Unexp LastUse Member key
__          0     0     0         CICSA.CATA
__          0     0     0         CICSA.CATD
__          0     0     0         CICSA.CDBD
__          0     0     0         CICSA.CDBF
__          0     0     0         CICSA.CDBO
__          0     0     0         CICSA.CDBQ
__          0     0     0         CICSA.CDTS
__          0     0     0         CICSA.CECI
__          0     0     0         CICSA.CEDA
__          0     0     0         CICSA.CEDF
__          0     0     0         CICSA.CEDX
__          2     0     0  1Apr09 CICSA.CEM%
__          0     0     0         CICSA.CESC
__          0     0     0         CICSA.CESD
__          0     0     0         CICSA.CEX2
__          0     0     0         CICSA.CFCL
```

Figure 498. RACLIST merged profile permits and UACC - Member profiles for selected Member class

In this detail view, you can see the individual member profiles. This information does not mean that the profiles are defined in the member class. These profiles can also be defined as members in a corresponding grouping class profile.

You can continue zooming in on report data to get details.

Reduced access information

In the Member profile detail view, the **Red** (Reduced Access) column indicates whether the access level shown for this userid or group is less than it would be if the specific ACL entry were absent. For example, the **Red** field contains `Yes` for an entry that shows a userid that was permitted READ access to a resource when the user also belongs to a group that has UPDATE access. In this example, the userid has the lower READ access because of the READ permit. If this ACL entry was removed, the user would have the higher UPDATE access based on the group membership.

```
RACLIST merged profile permits and UACC
Command ===> ____________________________________________________
 Permits by member, Member classes like %CICS*
   Allowed Deny  Unexp LastUse MemClass Complex
__        81     0     0 10Apr09 TCICSTRN SYS1
   Allowed Deny  Unexp LastUse Member key
__         2     0     0  1Apr09 CICSA.CEM%
   Allowed Deny  Unexp LastUse Permit   Access    Red Name
__        0     0     0         -UACC-   NONE      No
__        0     0     0         BCSGB02  READ      No  TEST USER
__        0     0     0         IBMUSER  READ      No  NAME
__        1     0     0  1Apr09 SYSAUDIT READ      No
__        1     0     0  1Apr09 SYSPROG  READ      No
******************************** Bottom of Data ******************
```

Figure 499. RACLIST merged profile permits and UACC report - Access list information for selected member profile

Notes on interpreting RACF Access Usage reports

- The `-UACC-` entry always has a high violation count. The high count is caused by the violations from all users that are not included on the access list or in any group on the access list. RACF first checks if the user has access to a resource by

checking the access list. If the access list does not allow or prevent access, RACF uses the UACC. Thus, the count on the -UACC- entry is typically rather high.

- Especially for the -UACC- entry, The report does not show the user or job that accessed or failed to access the resource. The fact that the UACC was used is an indicator that the user or group is not present on the access list. There is no option to zoom in to a level of detail that shows which user. If you need more information about this situation, set up an ACCESS report that selects the correct class and profile to show the users that accessed the resource.
- Some applications verify access to resources without actually using or accessing these resources. These access verifications are counted and reported in the RACF Usage reports. An example is an application that uses RACF access to determine the list of functions to be shown on a panel. The application performs this RACF access verification while suppressing all messages and auditing. After the user chooses an option, the application might do a second access check with auditing to record that the user has used the function. In contrast to SMF processing, the RACF Usage reports also include the initial verification process that is used to build the selection panel.
- Most reports include a column to indicate *reduced access*. This column indicates whether the access level shown for the userid or group is less than what it would be if the specific ACL entry were absent. For example, if a userid has been permitted READ access and at least one of the groups the userid is a member of has UPDATE access, the userid access reported is READ. However, if the specific permit for the userid is removed from the ACL, the access for the userid increases to UPDATE because of the group membership. In this example, the **Red** field for the entry where the READ access contains Yes to indicate that this permission represents reduced access.

Example: Reporting on Member usage

RACF administrators use RACF grouping resource classes and member lists because they allow a single access definition to be used for many different resources. These grouping resource profiles can include a long list of members. The members are used as if individual profiles had been defined in the corresponding non-grouping (or member) resource class. The use of grouping and member resource classes is described in the *RACF Security Server Administrator's Guide* (SA22-7683).

The use of grouping class profiles is transparent to the application that uses RACF functions to perform access verification. An application such as CICS or IMS checks access to the resource in the member class. For the entire process to work, the resource class must have been RACLISTed using either a SETROPTS RACLIST command, or by the application using a RACROUTE REQUEST=LIST statement. During the RACLIST process, information from the grouping class profiles and the member class profiles is merged. The application might have permitted access based on information coming from any of the profiles used during the merging. Consider this example where the following two grouping resource profiles have been defined:

```
GCICSTRN RESGRP1              GCICSTRN RESGRP2
Member CEMT                   Member CEMT
UACC   NONE                    UACC   NONE
ACL    USER1 READ             ACL    USER1 READ
                                     GRP1  READ
```

The userids used in this example are defined as follows:

```
USER1                 USER2
NAME     TEST  USER1  NAME     TESTUSER2
DFLTGRP  SYS1         DFLTGRP  SYS1
CONNECT  SYS1         CONNECT  SYS1,GRP1,GRP2
```

During the RACLISTing process, when all relevant profiles are merged into an in-storage table, the two grouping resource profiles are combined:

```
TCICSTRN CEMT  UACC  NONE
ACL      USER1        READ
         GRP1         READ
```

After RACLISTing the profiles, the information about which profiles were used to build the in-storage profiles is no longer available.

When USER1 accesses the CEMT transaction, access is permitted based on both the RESGRP1 and the RESGRP2 profiles.

When USER2 accesses the CEMT transaction access is permitted based on the RESGRP2 profile because USER2 is a member of GROUP GRP1, which has access.

As this example illustrates, it is not always immediately obvious which profile is used to allow or prevent access.

zSecure Admin provides a reporting function that matches the access request to the best fitting *in-storage* merged profile. For that profile, zSecure Admin shows those profiles that were used to build it.

For the CEMT transaction, the access of USER1 is based on information in profiles RESGRP1 and RESGRP2. For USER2, access is based on RESGRP2. The UACC is based on information in profile RESGRP1. Depending on which userid attempts to access a particular transaction, the access authority is based on different profiles. For non-grouping resource classes, like data sets, access for all users is always based on a single best-fitting profile. For RACLISTed grouping resource classes, the profile used is dependent on the userid.

The Member usage reports show the different access usage in an easy to understand multi-level format.

To begin reporting member usage, select option **AM.6** from the zSecure Admin main menu to open the report selection panel shown in the Figure 500 on page 668.

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
              zSecure Admin+Audit for RACF - Access - Member usage
Command ===> ____________________________________________________________

Show profiles that fit all of the following criteria:
Member class  . . . . . ________  (class or EGN mask)
Member key  . . . . . . _____________________________________________
Permit id . . . . . . . ________  (permit id or EGN mask on access list)
Complex . . . . . . . . ________  (complex or EGN mask)
Show accesses . . . . . _  Non-zero counts     _  Zero counts

Profile to use  2  1. Use historic profile name in access summary if present
                   2. Simulate access in database to find current profile

Advanced selection criteria
_  Further selection                    _  Date selection

Output/run options
_  Print format          Customize title     Send as email
      Background run     Full page form
```

Figure 500. Member Usage report selection panel

For information about setting up the report, see "Setting up and generating the reports" on page 660.

Example: Reporting on Global Access Checking

The data collected by the RACF Access monitor includes information indicating whether a particular access request was satisfied using the Global Access Checking (GAC) table. The GAC Table is used to improve performance for public resources. It has entries that permit all users to have access to a resource. Each entry also specifies the access level permitted. (See "*Setting Up the Global Access Checking Table*", *RACF Security Server Administrator's Guide* (SA22-7683).)

In zSecure Admin, two options are available to report on access permitted using the GAC: Access Summary report (**AM.1**) and the Global Access Checking Usage report (**AM.7**).

The Access Summary report provides an overview of all access requests to all resources that were permitted using the GAC Table. To include this information in the report, you must specify the advanced selection criteria option for global access checking on the Further selection panel. For details, see "Reporting on actual profile usage" on page 649.

The Global Access Checking Usage report provides an overview of access permitted using the GAC based on the currently defined entries in the GAC Table.

To begin reporting member usage, select option **AM.6** from the zSecure Admin main menu to open the report selection panel shown in the Figure 501 on page 669.

```
 Menu         Options       Info    Commands     Setup
──────────────────────────────────────────────────────────────────────────────
                          zSecure Admin+Audit for RACF - Access - Global usage
Command ===> ____________________________________________________________

Show GLOBAL profiles that fit all of the following criteria:
RACF profile name . . . ____________________________________
Permit id . . . . . . . ________  (permit id or EGN mask on access list)
Complex . . . . . . . . ________  (complex or EGN mask)
Show accesses . . . . . _ Non-zero counts     _ Zero counts

Profile to use  _ 1. Use historic profile name in access summary if present
                  2. Simulate access in database to find current profile

Advanced selection criteria
_ Further selection                   _ Date selection

Output/run options
_ Print format          Customize title     Send as email
    Background run
```

Figure 501. Member Usage report selection panel

You can set up the report to be generated based either on the actual historic use that has been made of the GAC Table or on a simulation using the current GAC Table. The history report uses the Access Monitor data and only reports on those access requests that were granted using the GAC table at the time of the access request. The simulate report analyzes all access requests and determines whether the current GAC table allows access. If the GAC Table has not been modified since the Access Monitor data was collected, the data in both reports is the same.

For information about setting up the report, see "Setting up and generating the reports" on page 660.

Reviewing the results

Figure 502 on page 670 shows Global Access Usage report results.

Use the Global Access Usage report to view the following types of information:

- A summary of access information for selected profiles categorized by result, (*allowed*, *denied*, and *unexplained* for example.
- Select an individual profile entry to view a summary of the access monitor information for that profile as shown in Figure 502 on page 670.
- In the profile view, select an individual access monitor record to view details about specific access events.

Figure 502 on page 670 shows a summary of the Global access table usage report for a specific profile.

```
Global access table usage
Command ===> ____________________________________________________
Global access table, All access monitor records
   Allowed Deny  Unexp LastUse Class    Profile
__     945     0     0 15Jun09 GLOBAL   DATASET
   Allowed Deny  Unexp LastUse Complex  Access  Member key
__       0           0         SYS1     ALTER   &RACGPID.**
__       0           0         SYS1     ALTER   &RACUID.**
__       0           0         SYS1     READ    AUT310.**
__       0           0         SYS1     READ    CSQ600.**
__     129           0 15Jun09 SYS1     READ    EOY.**
__      67           0 15Jun09 SYS1     READ    EUV.**
__     102           0 15Jun09 SYS1     READ    FAN140.**
__       0           0         SYS1     READ    FMN610.**
__       0           0         SYS1     READ    FMN710.**
__      13           0 10Jun09 SYS1     READ    GDDM.**
__      97           0 15Jun09 SYS1     READ    GIM.**
__       0           0         SYS1     READ    IGY340.**
__      90           0 15Jun09 SYS1     READ    IOE.**
__      61           0 10Jun09 SYS1     READ    ISF.**
__     173           0 15Jun09 SYS1     READ    ISP.**
__       4           0 10Jun09 SYS1     UPDATE  SYS1.BRODCAST
__     209           0 15Jun09 SYS1     READ    USER.**
*********************** Bottom of Data ***********************
```

Figure 502. Global access table usage report

In the example shown in Figure 502, you can find the following information:

- 945 access requests to the DATASET class were satisfied using the GAC Table. You can see similar information for other resource classes.
- The entry for &RACUID.** is empty because the Access Monitor was running with the default option NOINCLUDEOWNRESOURCE. If this option is enabled, all access attempts to data sets where the High-level qualifier matches the userid requesting access are suppressed from the Access Monitor data sets. These types of access requests typically show access requests to data sets specifically created for a given userid without providing any interesting information. Suppressing these records is done by default.

To view more detailed information about an access event, type **S** in the entry field for any entry.

Generating RACF usage reports using only RACF data

To run a report based on information from the current RACF database, you can use Access Monitor RACF reporting option AM.6 without specifying an Access Monitor data set. When the AM.6 report is run without an Access Monitor data set, the results include information based on the definitions in the RACF database only. Information about usage access, available in the Acccess Monitor collection reports, is not included. The following fields are not included in the report: **Allowed**, **Deny**, **Unexp** and **LastUse**.

Use the SETUP FILES function on the zSecure Admin main menu to remove the Access Monitor data sets from the selected set of input data sources. How you remove Access Monitor data sets depends on how they are setup. If you created a separate input file set for the Access Monitor data sets, clear the selection. If you added Access Monitor data sets to an existing data set, you can delete all lines that specify ACCESS in the **Type** column.

Performing RACF database cleanup tasks

Although removing unused or obsolete definitions might seem straightforward, the process is more complex in practice because resource profiles and access definitions can be unused or obsolete for many different reasons. For example, resource profiles and access lists might appear to be unused or empty, but on further investigation you might discover that they are used only under certain conditions. Because of this complexity, decisions about whether to delete profiles or modify access lists often require further analysis.

zSecure Admin provides several functions that can help identify and remove obsolete or superfluous definitions. However, most of these functions are based on a static analysis of the data in the RACF database. Sometimes the static analysis indicates that a profile, access list entry, or group membership is redundant. However, in reality the definition might have been used in the recent past, or it might be needed in the future.

zSecure Admin also provides functions that can help identify unused resource profiles and authorizations based on actual usage. These functions are based on dynamic analysis of the data in Access Monitor data sets. However, a purely dynamic analysis of the data might ignore the fact that some apparently unused definitions do serve a purpose. For example, if a profile prevents a user from accessing a resource, and the user never tried to access the resource, the profile shows up as unused. The user never created an access violation, but that does not mean that the corresponding access list entry is useless. It is only unused. The profile and the access list entry are still required to prevent future access attempts.

zSecure Admin provides several functions that correlate the data from the static analysis with the data from the dynamic analysis. Using this information, RACF administrators can confirm or deny the conclusions reached based on analysis of either type of data alone.

Most RACF cleanup activities require a combination of static RACF profile analysis and dynamic analysis of actual RACF profile use.

The following scenarios describe different types of RACF database cleanup tasks using examples of resource profiles and Access list definitions.

Scenario 1: Removing profiles that do not cover any resources or that duplicate other profiles

The following examples describe these types of profiles.

- A `DATASET` profile such as `<hlq>.data.**` has no data set matching that name. Such a profile might be leftover from a time when the data set existed. In that case, the profile can be deleted safely. The profile might also be one that is explicitly defined to describe a data set that is created occasionally and later deleted. In this scenario, further analysis is required before deciding to delete or retain the profile.
- A `DATASET` profile covers `<hlq>.test.**` and another `DATASET` profile covers `<hlq>.**`. With these two profiles, the first is a more specific profile that is only used for some data sets. The profile might have been created at some time and forgotten afterward. At the moment, this profile is not necessary because the `<hlq>.*` profile covers the same resources. Having both profiles can confuse system administrators or support personnel. Also, if an Administrator or Support person wanted to grant a group or user access to all `<hlq>` profiles, they would have to update two profiles instead of one.

Scenario 2: Removing profiles whose security contribution is unclear
The following example describes a profile that is a candidate for this type of RACF database cleanup.

A DATASET profile such as <hlq>.test.** exists at the same time as an almost identical profile, <hlq>.**. The only difference is that the first profile has one additional group or user on the access list. For this example, assume that the additional entry is C2XUSER. The access level permitted for C2XUSER might be higher or lower than it would have been if the entry were not in the access list. Because the more specific <hlq>.test.** profile might result in higher or lower access for C2XUSER using the more specific profile, further research is required to determine whether it is safe to delete the profile.

Scenario 3: Removing users or groups from the Access List for a resource profile
The following examples describes items that are targets for this type of RACF database cleanup.

- A user is a member of a group. Both the user and the group are on an access list with the same access level. In this situation, the user can be removed from the access list because the user access level granted is the same for the user entry and the group entry.
- A group is in the access list of a resource with the same access level as the level of either ID(*) or the UACC. The access list entry for the group can be removed because the group access level is the same whether permitted by the ID(*), the UACC, or the group.
- A user is in the access list of a resource with the same access level as the level of either ID(*) or the UACC. None of the groups for the userid are in the access list, and the user also does not have any group or system level OPERATIONS attribute. In this case, the access list entry for the user can be removed because the user access granted is the same for the user, ID(*) or the UACC.

Scenario 4: Evaluating group membership
The following example describes items that are targets for this type of RACF database cleanup.

Users can be a member of multiple groups. Through group membership, users can be permitted access to resources. Some of these groups might not be present in any access list when the user has only USE authority. Although such groups might be ineffective at the moment, they might have been used in the past or might be used in the future. Further analysis is required to determine whether the group can be safely removed.

Removing profiles

There are several categories of profiles that are candidates for deletion.

Redundant profiles
Redundant profiles are identical to the next higher level generic profile. zSecure Admin users can use the REPORT REDUNDANT and REPORT NONREDUNDANT functions to report on and automatically remove redundant profiles. These functions are available from the Cleanup option on the Access Monitor menu **(AM.9)**. You can also generate reports and remove redundant profiles through a batch job. For more information about the REPORT (NON)REDUNDANT function, see "RA.3.3 Redundant - Finding and removing redundant profiles" on page 205.

Empty profiles
Empty profiles do not protect any resources. zSecure Admin users can use the VERIFY NOTEMPTY function to report on empty profiles. This function is

available from the Cleanup option on the Access Monitor menu (**AM.9)**. You can also generate reports through a batch job. For more information about the VERIFY NOTEMPTY function, see "Removing unused generic profiles" on page 362. One problem presented by an empty profile is determining whether the data set profile is permanently empty. For example, the profile might apply to a data set that is created temporarily and then deleted. Before removing empty profiles, save the list and evaluate the list against profiles included in the *Unused profiles* report.

Unused profiles

Unused profiles are the most difficult type of profile to cleanup. These profiles often do protect resources, and their definition differs from the definition of the next higher generic profile. However, if the profiles are not used it might be worthwhile to investigate why the profiles exist and determine whether they can be removed.

Unused profiles are often higher level generic profiles that are hidden by more specific generic (or discrete) profiles. For example, given the following profile definitions, the top generic profile (SYS1.**) might be an empty, unused profile.

```
SYS1.**   UACC(NONE)   SYSPROG(ALTER)
SYS1.LINK*  UACC(NONE)   SYSPROG(ALTER)
SYS1.LPA*  UACC(NONE)   SYSPROG(ALTER)
...
```

All existing SYS1 data sets in the system are protected by one of the lower-level profiles, such as SYS1.LINK*. The lower-level profiles are used, but the top generic profile is unused. Such profiles are sometimes called backstop or catch-all profiles because they are only in place to cover resources not defined more specifically by other profiles. The REPORT REDUNDANT (**AM.9.2**) and VERIFY NOT EMPTY (**AM.9.3**) functions take this situation into account. These options leave the top generic profile in place and focus on the more specific profiles. They are available from the Cleanup option on the Access Monitor menu (**AM.9**).

Based on the discussion of redundant, empty, and unused profiles, you can see that only redundant profiles can be removed automatically. Decisions about removing all other profiles such as empty and unused ones require analysis and human judgment before the profile can be deleted. There are several approaches to deleting profiles which are described in the following sections.

Creating a strategy for profile removal

Before removing profiles, develop a strategy to identify which class of profiles to remove and how to remove them. The available options are different for data set profiles and for general resource profiles. For data sets, when you define a data set profile, you create profile can be used to allow the creation (allocation) of a data set on disk. For general resource profiles, the creation of the resource is typically not related to the existence of a matching profile. Also, for data sets, users can be authorized to create profiles based on their connection to a certain group. zSecure Admin provides some special functions to help remove data set profiles. These special functions are REMOVE REDUNDANT and VERIFY NOT EMPTY. You can use both these functions from the Cleanup option on the Access Monitor menu (**AM.9**).

When you remove profiles, you have two options:

1. Use a process that relies on the Administrator to analyze and remove profiles manually.

With this option, the Administrator first generates and analyzes profile usage reports (**AM.5**), and then generates a command to remove obsolete profiles. This process is the best and safest method for profile removal.

2. Run an automated process without analyzing profile usage.

   With this option, you rely on the zSecure Admin analysis to identify unused profiles and mark them for deletion. However, as described in "Removing profiles" on page 672, running the automated process without analyzing the profile usage might not always result in removal of the least useful profiles.

Removing data set profiles

You can remove profiles using a combination of automatic and manual actions that require administrator analysis and action. The following process The process requires the following steps which are described in this topic.

1. "Remove redundant profiles."
2. "Analyze profile usage."
3. "Check for empty profiles" on page 676.
4. "Identify almost redundant profiles" on page 676.
5. "Remove obsolete profiles" on page 676.

Note: When you use the Access Monitor reporting functions, verify that the Access Monitor data sets you designate as data sources cover a time period that is long enough for you to decide with confidence that the profiles are never used.

Step 1: Remove redundant profiles

1. On the zSecure Admin command line, type **AM.9**. Then, press **Enter** to open the Access Monitor Cleanup menu.
2. Select **2 Dataset** to open the Reports Redundant panel to specify the selection criteria to target the redundant profiles that you want to delete. (For field help, press F1.)
3. Enter a / in **Remove redundant profiles** to generate the delete commands for the redundant profiles.
4. On the command panel, follow the instructions at the top of the panel to run the commands.

Step 2: Analyze profile usage

After removing the redundant profiles, the next step is to analyze unused profiles to determine which profiles can be removed safely.

1. On the command line, type **AM.9.5** and press enter to open the Profile usage panel.
2. To report on unused profiles, enter a / in **Zero counts** as shown in Figure 503 on page 675.

```
 Menu         Options       Info    Commands     Setup
 ──────────────────────────────────────────────────────────────────────────────
               zSecure Admin+Audit for RACF - Access - Profile usage
Command ===> ____________________________________________________________

Show profiles that fit all of the following criteria:
Class . . . . . . . . . DATASET   (class or EGN mask)
RACF profile name . . . ________________________________________________
Permit id . . . . . . . ________  (permit id or EGN mask on access list)
Complex . . . . . . . . ________  (complex or EGN mask)
Show accesses . . . . . _  Non-zero counts     /  Zero counts

Profile to use  2  1. Use historic profile name in access summary if present
                   2. Simulate access in database to find current profile

Advanced selection criteria
_  Further selection                    _  Date selection

Output/run options
_  Print format          Customize title     Send as email
     Background run
```

Figure 503. Profile Usage report - Selection Criteria for reporting on unused data set profiles

3. Specify any other report selection criteria required. (See "Reporting on RACF Usage" on page 658 for more information about generating reports.)
4. After entering the report selection criteria, press **Enter** to generate the report.

Figure 504 shows an example of the resulting Profile Usage report.

```
Profiles, by class complex                                      Line 1 of 1
Command ===> ____________________________________________________ Scroll===> CSR
Profile usage, zero counts                                    18 Jun 2009 06:31
   Class    Complex    Prof  Permits  Missing
   DATASET  SYS1       106      804       18
   Type     Profile
__ GENERIC  AOP.**
__ GENERIC  APS330.**
__ GENERIC  ASU.**
__ GENERIC  AUT220.**
__ GENERIC  AUT230.**
__ GENERIC  BCSC.P.B8R112.**
__ GENERIC  BCSC.PLX370.**
__ GENERIC  BCSC.RACFDS.ZTM
__ MODEL    BCSC.TEST.GDGBASE
__ MODEL    BCCG011.MODEL.DSN
__ GENERIC  BCCG011.TEST.DATA
__ MODEL    BCSCGB3.MODEL
__ NONVSAM  BCSCGB3.TEST.DATA2
__ GENERIC  BCSCWN2.**
__ GENERIC  BIP210.**
__ GENERIC  BIP501.**
__ GENERIC  CDS.**
```

Figure 504. Profile Usage report showing unused data set profiles

This report shows all the data set profiles that have not been used for the time period for which access monitor records are available. If the report shows too many profiles, you can apply additional selection criteria to limit the results. For example, you can specify a data set name pattern. Selecting records based on user-specified criteria allows you to focus on selected profiles during the analysis. You can also use the **Advanced Selection** criteria. For example, you might specify profile creation date criteria to limit the report to the oldest profiles.

Use the **S** line command to review details of a particular profile in the report. For example, selecting the ASU.** profile in Figure 504 on page 675 opens the detail view shown in Figure 505.

```
Profiles, by class complex                                      Line 1 of 1
 Command ===> _____________________________________________ Scroll===> CSR
Profile usage, Classes like DATASET zero counts
    Class    Complex  Prof  Permits  Missing
    DATASET  SYS1       106      804      18
    Type     Profile
    GENERIC  ASU.**


    Profile in current database
    Security complex name         SYS1
    RACF profile class            DATASET
    Profile type                  GENERIC
    RACF profile name             ASU.**
    Volume serial
    Permits and UACC              3

    Profile usage statistics
    Allowed                       0
    Deny                          0
    Unexp                         0
    Last use in access summary
```

Figure 505. Profile Usage report showing unused data set profiles

From this example, you can see that a total of three permits (including the UACC) have been permitted for this profile. The Profile usage statistics in this example also show that the profile has not been used during the measurement period.

Step 3: Check for empty profiles

After reviewing the profile usage information, the next step is to determine whether the unused profiles are empty.

1. On the command line, type **AM.9.3** and press **Enter** to open the Access Monitor Cleanup menu.
2. To identify profiles that are good candidates for removal, look for those profiles that are also included in the Profile Usage report for unused profiles

Step 4: Identify almost redundant profiles

After checking for empty profiles, the next step is to determine whether a profile is an almost redundant profile and analyze the reasons that it is not redundant. For more information about non-redundancy, see "RA.3.3 Redundant - Finding and removing redundant profiles" on page 205.

Step 5: Remove the obsolete profiles

For each profile identified in the analysis process, issue a RACF DELDSD command to delete the profile.

This same removal process can also be followed by running the Report redundant report (**AM.9.2**) or Verify Not Empty report (**AM.9.3**) first. After running these reports, generate the Profile Usage report for unused profiles and compare the results to the Redundant and Verify Not Empty reports to identify profiles that need to be removed.

Removing general resource profiles

The process for removing unused general resource profiles is different than the process for removing data set profiles. For example, zSecure Admin does not provide any function to verify that CICS, IMS, or DB2 resource profiles actually

match any resources for those subsystems. Consequently, you have to use another process to evaluate the usefulness of these general resource profiles. zSecure Admin does report about usage of these profiles, but the final decision about removing profiles must be made using additional criteria. Figure 506 shows a Profile Usage report with a list of unused general resource profiles by class.

```
Profiles, by class complex              6 s elapsed, 5.3 s CPU
Command ===> _____________________________________________ Scroll===> CSR
Profile usage, zero counts                      18 Jun 2009 12:51
Class    Complex  Prof  Permits  Missing
__ ACICSPCT SYS1         3        4       0
__ AIMS     SYS1         1        1       0
__ CBIND    SYS1         2        5       1
__ CIMS     SYS1         1        1       0
__ DATASET  SYS1        81      805      13
__ DCICSDCT SYS1         3        6       0
__ DSNR     SYS1        38       81       0
__ FACILITY SYS1        30      200      22
__ GCICSTRN SYS1         2       16       1
__ GMBR     SYS1         1        2       0
__ GXFACILI SYS1         1        6       4
__ JESINPUT SYS1         1        3       0
__ JESSPOOL SYS1         1        7       3
__ OPERCMDS SYS1         7       38       0
__ PMBR     SYS1         1        1       0
__ PTKTDATA SYS1         2        9       0
__ RACFEVNT SYS1         4        5       0
```

Figure 506. Profile Usage - Unused general resource profile report

Use the **S** line command to review detailed profile information for any class. Figure 507 shows the detail view for the GCICSTRN class.

```
Profiles, by class complex                      Line 1 of 2
Command ===> _____________________________________________ Scroll===> CSR
Profile usage, zero counts                      18 Jun 2009 12:51
   Class    Complex  Prof  Permits  Missing
   GCICSTRN SYS1         2       16       1
   Type     Profile
__  GROUPING CICSA.STST
__  GROUPING CICSA.TEST
****************************** Bottom of Data ********************************
```

Figure 507. Profile Usage report - Profiles by class detail view

After identifying potential unused profiles in the Profile Usage report, you can analyze the profiles to determine which ones need to be removed. If the results of the analysis indicate that a profile needs to be deleted, the administrator can issue the necessary RACF RDELETE commands to delete the profile.

Automatically removing unused profiles

You can automatically generate the applicable remove commands to remove unused profiles in a single step using the Access Monitor Remove Profiles option (**AM.8.1**). Using the automated process offers two significant benefits: the remove commands can be automatically generated based on user-specified selection criteria, and a recovery command file is automatically generated that can be used to restore profiles that have been removed in error.

When you run the recovery command file, profiles are restored to their original state. Some characteristics such as the creation date are different, but otherwise the recovered profiles are identical. For data set and general resource profile cleanup, the number of recovery commands generated is typically significantly larger than

the number of delete commands. This increase occurs because additional alter and permit commands are often required in addition to the define command for the profile.

Notes:

1. When using the automatic profile removal process, you must specify a matching CKFREEZE file in the data sources you specified using SETUP FILES. (See "SE.1 Setup - Input files" on page 1645). Without a matching CKFREEZE file, either the recovery file might be incomplete, or the ACL removal file might contain incorrect commands.
2. Automatic profile removal only works when exactly one RACF data source is selected in SETUP FILES. If more then one RACF data source is selected, an error message is issued.

Generating remove (delete) and recovery commands:

1. From the AM monitor menu, type AM.8 to open the Remove panel shown in Figure 508.

```
                  zSecure Suite - Access - Remove
Option ===> ____________________________________________


1    Profiles        Remove unused profiles
2    Permits         Remove unused permits
3    Connects        Remove unused connects

Recovery command file
BCCG011.RECOVERY.CKRCMD_____________
```

Figure 508. Access Remove unused profiles, permits, and connects panel

2. In the **Recovery command file** field, type the name of a permanent data set to save the recovery commands.

   The recovery command file is overwritten each time a Remove operation is performed. If you want to save recovery command files from previous remove operations, specify a new data set name for each recovery operation.
3. Select the Remove option required.
4. On the Remove selection criteria panel, specify the selection criteria for items you want to remove. Use the Advanced Selection criteria options if necessary.
5. Press **Enter** to generate the commands.

Removing access and connects

Other types of information that you might want to remove are access list entries and group connections that are not being used. zSecure Admin provides an independent cleanup function to remove all userid-based access list entries that are unnecessary. Running this Remove Redundant Permits function first results in a more complete cleanup of the access list entries.

During the access verification process, RACF checks whether the userid that is requesting access is included on the access list. If the userid is present, RACF grants or denies access based on that access list entry. In this situation, group-membership is not considered. This same approach is used by zSecure Admin to determine which ACL entries are used. This processing logic means that if a user has the same access that is granted through one of its groups, the group access is not considered, and all access is counted towards the userid ACL entry. As a result, the ACL entry for the userid is classified as used and the ACL entry

for the group is classified as unused. Because access control through groups is the preferred method, counting on these redundant userid-ACL entries is undesirable. To remove these confusing and unnecessary ACL entries and enable proper counting of the use of group-related ACL entries, run the Remove Redundant Permits function at the beginning of the cleanup process

After you remove redundant permits, you can analyze and remove unused permits and connects. For details, see the following sections.

- "Removing redundant permits"
- "Manually remove unused permits"
- "Automatically removing unused permits" on page 681
- "Manually remove unused connects" on page 681
- "Automatically removing unused connects" on page 683

Removing redundant permits

Redundant permits are those permits that provide the same level of access that a user already has through membership in a group. In this case, removing the user from the access list results in RACF using the highest access permitted by the user's connect groups. If the access is the same, the access permitted using the specific user ID ACL entry is considered a *redundant permit*. Removing redundant permits can typically be done without any adverse effect.

1. On the command line, type **AM.9.2** and press **Enter** to generate the commands to remove the redundant permits.
2. On the command panel, follow the instructions at the top of the panel to run the commands.

For additional information about removing redundant permits see the REDUNDANT_PERMIT keyword in "REMOVE" on page 870.

Manually remove unused permits

The following process demonstrates how to remove unused access list (ACL) entries manually based on administrative analysis. Verify that the Access Monitor data sets you designate as data sources cover a time period that is long enough for you to declare an entry as obsolete. (See "Setting up zSecure to analyze and report on Access Monitor data" on page 647.)

Step 1. Review unused ACL entries.

Step 2. Verify that ACL entries are not being used.

Step 3. Delete the unused ACL entries.

Step 1: Reviewing unused ACL entries

1. On the command line, type **AM.3** and press **Enter** to open the Permit usage panel.
2. To report on unused connects, enter a / in the **Zero counts** field.
3. Specify any other report selection criteria required. (See "Reporting on RACF Usage" on page 658 for details about specifying selection criteria.)

   If you want to remove almost unused ACL entries, or want to remove ACL entries that have not been used for a long time (stale entries), select the applicable **Advanced selection criteria**.
4. After entering the report selection criteria, press **Enter** to generate the report.

Step 2: Verifying that ACL entries are not being used

On the Permit Usage report, you can review the unused ACL entries by using the **S** line command for the class you are interested in. Figure 509 shows the ACL entries for the FACILITY class.

```
Unconditional permits and UACC, by class complex/profile
Command ===>  ____________________________________________________
Permit and UACC usage, zero counts
   Allowed Deny  Unexp LastUse Class    Complex
__       0     0     0         FACILITY SYS1
   Allowed Deny  Unexp LastUse Type     Profile
__       0     0     0         DISCRETE STGADMIN.EDG.LIST
   Allowed Deny  Unexp LastUse Id       Access    Used    Failed  Red RdM
__       0     0     0         -UACC-   NONE                      No
__       0     0     0         DFHSM    READ                      Yes
__       0     0     0         IBMUSER  ALTER                     No
__       0     0     0         SYSPROG  UPDATE                    No
__       0     0     0         SYS1     ALTER                     No
****************************** Bottom of Data ******************************
```

Figure 509. Permit Usage report - Unused permits for a selected class

Evaluate the individual ACL entries using your knowledge of the environment and the information provided by the **Red** and **RdM** columns.

Red field

The **Red** column indicates whether the ACL listed in the panel reduces the access level for the specified user or group ID. If the value is *Yes*, the ACL grants a lower access level than the access that would be granted if the ACL entry was removed. For example, in Figure 509 the `DFHSM` userid has READ access to the FACILITY class profile shown (*SYS1*). If this ACL entry is removed, the userid `DFHSM`, which is probably used to run the started task for DFSMShsm, has a higher access.

Entries that have *Yes* in the **Red** field require further investigation to determine whether an ACL entry can be safely removed. To investigate, you can run a RACF `Listuser DFHSM` command to determine group membership for the userid and access level granted by each group identified. In this example, the investigation determines that the userid `DFHSM` is a member of the group `SYSPROG`. Figure 509 shows that the SYSPROG group has UPDATE access. So if the ACL entry is removed, the effective access level for the userid `DFHSM` changes to UPDATE which might allow a higher access level than intended.

RdM field

Like the **Red** field, the **RdM** column indicates that the ACL entry represented reduces the access level for the specified ID. The **RdM** field value is *Yes* if the access shown is less than the access granted through an ACL entry in another profile which is merged with the current profile during the RACLIST process.

Entries that have *Yes* in the **RdM** field require further investigation to determine whether the ACL entry can be safely removed.

You can also use the **S** line command to view the details for a particular ACL entry. On the resulting display, use the **L** line command to run the appropriate RACF LIST command for the userid or group.

Step 3: Removing unused ACL entries

After verifying that an ACL entry is not being used, you can use the **D** line command to delete it.

1. In the line command area for the entries you want to delete, type **D**.
2. Press **Enter** to generate the commands.

3. On the Confirm panel, verify and edit the commands as required, and set the mode to run the commands.

   If you want to be able to restore deleted ACL entries, use the automatic deletion method for the ACL entries you identified for deletion during your analysis.

Automatically removing unused permits

You can automatically generate the applicable delete commands to remove unused permits in a single step using the Access Monitor Remove Permits option (**AM.8.2**). The automated process offers several significant benefits:

- Automatic generation of the delete commands based on user-specified selection criteria including the creation date of the profile and the usage dates of the ACL entry.
- Automatic generation of a recovery command file to re-establish the access list entries that are deleted.
- You do not need to visually inspect every `Red` and `RdM` flag setting.
- Commands are generated to reset the UACC to NONE.
- You can generate multiple delete commands in a single operation.

In the absence of any selection criteria, all unused ACL entries are selected for deletion. The universal access (UACC) is handled like regular ACL entries. The UACC is represented by the pseudo ID `-UACC-`, and the generated commands are ALTDSD and RALTER.

Note: When using the automatic deletion process, you must also specify a matching CKFREEZE file in the data sources you selected using SETUP FILES. (See "SE.1 Setup - Input files" on page 1645.) Without a matching CKFREEZE file, either the recovery file might be incomplete, or the ACL removal file might contain incorrect commands.

Manually remove unused connects

The following process demonstrates how to remove unused connects manually based on administrator analysis and action. Make sure that you have collected sufficient usage information to declare an entry as unused. Before removing any access, verify that the Access Monitor data sets you designated as data sources cover the time period that you intended. (See "Setting up zSecure to analyze and report on Access Monitor data" on page 647.)

Step 1. Review unused connects.

Step 2. Verify that group connections are not being used.

Step 3. Delete the unused connects.

Step 1: Reviewing unused connects

1. On the command line, type **AM.4** and press **Enter** to open the Connect usage panel.
2. To report on unused connects, enter a / in the **Zero counts** field.
3. Specify any other report selection criteria required. (See "Reporting on RACF Usage" on page 658 for details on specifying selection criteria.)

   If you want to remove *almost unused* connects or connects that have not been used for a long time (stale connects), select the Advanced Criteria options to specify the applicable selection criteria to report on these types of connects.
4. After entering the report selection criteria, press **Enter** to generate the report. Figure 510 on page 682 shows a Connect Usage report with a list of

unused connects.

```
Connect authority use, by group
Command ===> _____________________________________________
Connect usage, zero counts
Allowed Deny  Unexp LastUse Group    Complex  InstData
__   0     0     0          #EMPLOY  SYS1
__   0     0     0          #READ    SYS1
__   0     0     0          ADB210   SYS1
__   0     0     0          ADCD     SYS1
__   0     0     0          AOP      SYS1
__   0     0     0          APS330   SYS1
__   0     0     0          ASU      SYS1
__   0     0     0          AUT220   SYS1
__   0     0     0          AUT230   SYS1
__   0     0     0          CMDTEST  SYS1
__   0     0     0          CRMA     SYS1
__   0     0     0          CRMB     SYS1
__   0     0     0          C2RSERVG SYS1
__   0     0     0          C2XGRP   SYS1
```

Figure 510. Connect Usage report - Unused connects

Step 2: Verify that group connections are not being used

The Access Monitor program only records regular access verification requests. Consequently, the use of group connections for other purposes is not recorded. For example, a group connection can also be used to define new data sets and new data set profiles to connect users to the group and even to define new groups. Most of these actions are not recorded by the Access Monitor program.

Before deleting unused connections from the unused connect list, you must verify that the group connections in the list are not being used. The authorizations required for group connections being used for unrecorded actions typically involve either a group connect-authorization higher than USE, or a non-default connect-attribute, like group-special or group-operations. You can review the connect authorization for group connects and the connect attributes for users from the Connect Usage report.

1. On the Connect Usage report, type **S** in the line command area for a group connect entry.
2. Press **Enter** to see the detailed information for the group connection as illustrated in Figure 511.

```
 Connect authority use, by group
Command ===> _____________________________________________
Connect usage, zero counts
    Allowed Deny  Unexp LastUse Group    Complex  InstData
__        0     0     0         SYS1     SYS1
    Allowed Deny  Unexp LastUse Userid   Access  Name                RI DfltGrp
__        0     0     0         BPXOINIT USE     BPXOINIT               SYS1
__        0     0     0         CICSDFLT USE     CICS DEFAULT         Y SYS1
__        0     0     0         CICSUSER USE                            SYS1
__        0     0     0         DB8GRFSH USE                            SYS1
__        0     0     0         DB9GENV5 USE                          Y SYS1
__        0     0     0         DB9GRFSH USE                          Y SYS1
__        0     0     0         DSN1WLM1 USE                            SYS1
__        0     0     0         FTPD     USE     FTPD                   SYS1
__        0     0     0         IBMUSER  JOIN    NAME                Y  SYS1
__        0     0     0         IMS71CR1 USE     IMS                  Y SYS1
__        0     0     0         IMS71DL1 USE     IMS                  Y SYS1
```

Figure 511. Connect Usage report - Connect authority use by group detail view

In this example, the SYS1 group includes the user IBMUSER with JOIN authorization. Because this authorization level is higher than USE, this group connection is not a good candidate for removal. The display also shows the default group (DFLTGRP) for the userid. The default group cannot be removed from a userid.

3. To determine whether a userid has a non-default group-attribute, use the **S** line command to view the detailed user information. Then, use the **L** command to LIST the userid profile. If the user to group connections show any non-default attribute, carefully evaluate how the connect is used before deciding to delete it.

Step 3: Remove the unused connects

After verifying that a connection is unused, use the **D** line command to delete it from the Connect Usage detail view shown in Figure 511 on page 682.

1. In the line command area for the entries you want to delete, type **D**.
2. Press **Enter** to generate the commands.
3. On the Confirm panel, verify and edit the commands as required and set the mode to run the commands.

   If you want to be able restore the connects after removal, you might want to use the automatic removal method.

Automatically removing unused connects

You can automatically generate the applicable remove commands to remove unused connects in a single step using the Access Monitor Remove Connects option (**AM.8.3**). Using the automated process offers several significant benefits:

- Automatic generation of the remove commands based on user-specified selection criteria.
- Automatic generation of a recovery command file to restore connects that have been removed if required.
- You do not have to visually inspect every connect to be removed.
- You can generate multiple remove commands in a single operation.

Note: zSecure Access Monitor does not collect access information for Unix directories and files inside zFS and HFS files systems. RACF connect groups that are only used for access to Unix files are therefore not detected as being used. Such RACF groups are included in the command files for connect removal. Before running the generated commands, verify that no connections required for access to Unix files are removed.

When you use the automatic connect removal process, USE level group-connections with default group-attributes that have not been used during the recorded period are deleted. The Advanced selection criteria allow selection on the connection of the user to the group and selection on the usage dates of the connect. In the absence of any selection criteria, all unused group connections are selected for deletion.

Note: When using the automatic connect removal process, you must also specify a matching CKFREEZE file in the data sources that you specified using SETUP FILES. (See “SE.1 Setup - Input files” on page 1645). Without a matching CKFREEZE file, either the recovery file might be incomplete, or the connect removal file might contain incorrect commands.

Consolidating data collected by Access Monitor

Table 277 describes the different types of Access Monitor consolidation data sets that can be used in Access Monitor reporting and database cleanup activities.

Table 277. Access Monitor program - consolidation data set types

Type of consolidation data set	Description
Daily consolidation data set	Access Monitor automatically collects access event data at a defined SMF interval (the default is 30 minutes) and writes the data to a data set. The SMF interval is defined by the INTVAL parameter in member SMFPRMxx in PARMLIB. At the end of the day, these data sets are consolidated into a single data set. This consolidation summarizes similar data within the collection data sets for each interval. The individual data sets created for each interval during the day are deleted. As part of the consolidation process, all records for similar events are combined and counted together. In the combined record, only the date and time of the last occurrence for each event is kept.
Consolidation data set for installation-defined interval (weekly, bi-weekly, or monthly)	An installation can define a manual or automated task to summarize similar data within the consolidated daily files. Then, the summarized data can be written to a file containing weekly, bi-weekly, or monthly data, for example. The main purpose for this secondary consolidation is to reduce the file size and processing time required to generate reports. However, this type of consolidation can result in a loss of detailed event information. For example, if consolidation is done in a monthly file, the resulting reports cannot be used to determine whether a user accessed a particular resource two weeks ago. The monthly consolidation process only retains information about the last file access for the month, not a week within the month.
User-created consolidation data sets.	Users can create their own Access Monitor data sets by submitting a batch job that consolidates existing data sets. For example, if the Access Monitor program has been configured to create daily and monthly consolidation data sets. A user who wanted a weekly consolidation data set can create one by consolidating the daily data sets for a given week.

The type of consolidation sets available in your installation depend on the configuration options selected during installation and deployment. The sample jobs provided with zSecure Admin use a monthly consolidation scheme.

During the monthly consolidation process, the existing daily files are deleted. Your installation might decide to run the monthly process in the second half of the month to retain detail information for a longer period. A second step in the sample job consolidates the last 12 months of data into a single file. The data set names in the sample jobs use the following naming conventions:

```
-hlq-.C2PACMON.Dyymmdd.Thhmm  30-minute interval
-hlq-.C2PACMON.Dyymmdd     Daily consolidation file
-hlq-.C2PACMON.Myymm     Monthly consolidation file
-hlq-.C2PACMON.Y12mon     Last-12-months consolidation file
```

If the sample consolidation process is implemented, the consolidation data sets for the installation will be like the ones shown in the following examples.

Daily consolidation files

```
03-Dec 2008   <hlq>.C2PACMON.D081203
02-Dec 2008   <hlq>.C2PACMON.D081202
01-Dec 2008   <hlq>.C2PACMON.D081201
```

Monthly and yearly consolidation files

```
                Monthly file      Yearly file
01-Nov 2008 - 30 Nov 2008   <hlq>.C2PACMON.M0811  <hlq>.C2PACMON.Y12MON
```

For instructions to set up the daily and monthly consolidation processes for your site, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

You can perform a manual consolidation using a job like the sample job C2PJCOND provided in the SCKRSAMP data set. The sample job assumes that the output data set exists. After successful processing, it deletes the data sets fed into the consolidation process. To run your own consolidation, you must create the output Access Monitor data set and specify the data sets to be fed into the consolidation process without the DELETE option as shown in the following code sample.

```
//CKRCARLA EXEC PGM=CKRCARLA,REGION=64M
//STEPLIB  DD DISP=SHR,DSN=&CPREFIX..SCKRLOAD
//C2PACMON DD DSN=your.output.accmon.dataset,
//            DISP=(MOD,CATLG),VOL=SER=&VOLSER.,
//            SPACE=(CYL,(1,1)),
//            RECFM=VB,LRECL=584,BLKSIZE=27998
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DATA,DLM=##
ALLOC TYPE=ACCESS DSN=your.input.accmon.dataset
ALLOC TYPE=OUTPUT DD=C2PACMON
include dd=sckrcarl member=c2pamcon
##
//SCKRCARL DD DISP=SHR,DSN=&CPREFIX..SCKRCARL
```

Figure 512. Sample JCL for consolidating Access Monitor data

You can repeat the `ALLOC TYPE=ACCESS` statement for as many data sets as needed. Alternatively, you can use DSNPREF to specify the prefix of all data sets that need to be consolidated. This sample job uses standard CARLa script to perform access monitor data consolidation (`C2PAMCON`). If you want to apply the consolidation to a subset of the input records, you can code your own version of this CARLa script, using appropriate SELECT statements. (See Chapter 12, “CARLa Command Language,” on page 713.)

Data reduction of Access Monitor data

The daily, monthly and yearly consolidation process as described in “Daily collection and consolidation” on page 646 combines multiple records for similar events into a single record. During this process, information about the exact moment at which the events occurred is discarded. Only the timestamp of the last occurrence is kept in the single output record. The counters for the number of times that the event occurred are added together and also kept in the single record. This method of combining multiple records is called consolidation. Hardly any information is lost.

For some situations, the consolidation process is not efficient. For example, every day a data set is created and used and the data set name has a qualifier with

today's date. While logically all these data sets belong together, the Access Monitor records for those data sets are not consolidated across multiple days. Another example is the use of Generation Data Groups (GDGs). Every generation data set within the group has a unique name. In RACF, the generation number is often irrelevant, but because of the different last qualifier the Access Monitor records are not consolidated for the entire generation data group. zSecure Admin provides several functions to process and discard part of resource names and other fields in the Access Monitor records. Use of these functions is called data reduction. Some information about the original event is permanently lost.

Several common data reduction methods can be invoked using built-in support for specific data set resources. Unless overruled during installation and deployment of Access Monitor, these common data reduction methods are applied during the automatic daily consolidation process. The available common data reduction functions are as follows:

SUPPRESS ACCESS_GDG_VERSION
The last qualifier of generation data sets is mapped onto GnnnnVnn.

SUPPRESS ACCESS_JESSPOOL_JOBID
The JOBID qualifier of JESSPOOL profiles (4th qualifier) is mapped onto Sxxxxxxx, Jxxxxxxx or Txxxxxxx, depending on the first character of the qualifier.

SUPPRESS ACCESS_JESSPOOL_DSID
The DSID qualifier of JESSPOOL profiles (5th qualifier) is mapped onto Dxxxxxxx if the first character of the qualifier is the character D.

It is also possible to perform more advanced data reduction using the CONVERSION statement as described in section “CONVERSION” on page 737. An example of such data reduction is shown in the following CARLa example.

```
conv type=access date3 replchar((substr(qual3,2,8),'d')),
     where (class=dataset,
            qualnum(resource)=4,
            qualif(resource,2)='C2PACMON',
            substr(qualif(resource,3),1,1)='D')
conv type=access time4 replchar((substr(qual4,2,8),'t')),
     where (class=dataset,
            qualnum(resource)=4,
            qualif(resource,2)='C2PACMON',
            substr(qualif(resource,4),1,1)='T')
...
 summary ,
...
 resource(0 l1char conv(date3,time4)) | ,
...
```

Figure 513. Data reduction example using CARLa CONVERSION statement

In this example, the conversion rules date3 and time 4 are defined. The intention is to apply data reduction to data set names with the following pattern:

```
HLQ.C2PACMON.D110819.T1556
```

The rules are rather simple and assume that all resources of type DATASETS with 4 qualifiers, with the second qualifier equal to C2PACMON, and the third qualifier starting with a "D", or the fourth qualifier starting with a "T" should be combined. In the target field, the rest of that third or fourth qualifier is replaced by lowercase "d" and "t".

In the WHERE clause, the conversion rules test the contents of the CLASS field and the format of the RESOURCE field, but the conversion rules do not specify which field should be the target of the data reduction. They only specify the method of data reduction. The target field of the data reduction is decided by the use of the CONV specification in the fields that are included in the SUMMARY statement. In this example, this is also the RESOURCE field. When used on the RESOURCE field, the dsname shown before is reduced to:

```
HLQ.C2PACMON.Ddddddd.Ttttt
```

Because the dsname now has no date and time specific information, the records for this resource can be consolidated with those for other dates or times. The original dsname is not available in the consolidated records.

Data reduction as specified in member C2PAMMAP in the SCKRCARL library occurs automatically during the daily consolidation. If you want to perform manual data reduction you can make a copy of the C2PAMMAP and C2PAMCMP members and use them in a job similar to the one shown in Figure 513 on page 686. Change the data set name and the include statement to match your setup. The C2PAMCMP member also uses the POE and JOBNAME selections currently configured in the parameter library. The ddnames C2PAMJOB, C2PAMRCL, and C2PAMPCL should point to data sets that contain applicable data, as described in "Configuring Jobname and POE-data collection" on page 646.

Converting Access Monitor Data

Access Monitor records can be in two different formats. The first format is the one used in zSecure Access Monitor for V1.12 and earlier releases. This format was introduced in zSecure V1.11, and is called the V1.11 format. The other format is the one introduced in zSecure Access Monitor V1.13, this format is called the V1.13 format. The benefit of the V1.13 format is that it allows for a much faster consolidation by processing all input files in parallel. All sample CARLa members in SCKRCARL and SC2PSAMP create data using the V1.13 format.

For reporting and analysis purposes, you can use any combination of V1.11 format and V1.13 format data.

If you want to consolidate existing Access Monitor data in V1.11 format, you cannot use CARLa member C2PAMCON. Before consolidating, V1.11 format data must be converted to the V1.13 format. You can do the conversion using the same procedure as outlined in "Data reduction of Access Monitor data" on page 685. The data reduction process can use any combination of V1.11 format and V1.13 format data, and always creates data using the V1.13 format. It is also possible to do the conversion using a simpler CARLa that does not perform any data reduction. Member C2PAMCVT in SCKRSAMP is provided for this purpose. It does not specify any data reduction, but only performs a direct conversion to the V1.13 format. The output is written to DDNAME C2PACMON. Use this CARLa in a job similar to the one shown in Figure 513 on page 686. Change the Access Monitor data set names and specify member C2PAMCVT in the include statement.

The conversion process can require a significant amount of CPU time and virtual storage, similar to the consolidation process used in zSecure V1.12 and earlier releases. If the required virtual storage is more than what's available, you can split the conversion process into smaller parts. This requires adapting the CARLa as provided in C2PAMCVT. Make a copy of this member and insert applicable CARLa SELECT and EXCLUDE statements to define subsets of Access Monitor records. For example one subset could be all records for CLASS=DATASET,

another for CLASS=JESSPOOL, and a third for all other classes. Another method could be to define the subsets based on userid ranges or resource name ranges. Use separate jobs or job steps to run conversion process on the defined subsets of Access Monitor records. Next use the regular consolidation process (for example using C2PAMCON) to consolidate the converted subsets into a single data set containing all converted records.

Chapter 11. Calling zSecure

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	

Note: If the RACF database is shared between z/VM and z/OS systems, perform all RACF administration and auditing functions using zSecure for the z/OS system. RACF on z/VM does not support some profiles, segments, and fields in the RACF database. As a result, you can create errors in the database if you change, copy, or recreate profiles from Tivoli zSecure Manager for RACF z/VM. You can use zSecure for z/OS to work with any profile in the shared database because z/OS supports all profiles, segments and fields in the RACF database, including fields like `VMMDISK` that are specific to z/VM.

If your database is shared, use the following procedure to capture the information from the z/VM system and analyze it using zSecure on the z/OS system.

1. Use Tivoli zSecure Manager for RACF z/VM to create and update a `CKFREEZE` file from the z/VM system.
2. Transfer the `CKFREEZE` file to the z/OS system for RACF administration and auditing.

You can call IBM Security zSecure for z/OS from the environments listed in Table 278. Other environments are not supported.

Table 278. Supported environments

Supported Environment	**For more information, see...**
ISPF in TSO	"Starting the interactive component" on page 9
Batch	"Starting zSecure programs using JCL" on page 690
TSO outside of ISPF and in Batch	"Starting zSecure through line mode commands" on page 696
z/OS UNIX System Services	"Starting zSecure through line mode commands" on page 696
CICS is only supported by zSecure CICS Toolkit	*IBM Security zSecure CICS Toolkit: User Guide*
IBM Tivoli zSecure Manager for RACF z/VM is only supported on z/VM systems	*IBM Tivoli zSecure Manager for RACF z/VM: User Reference Manual*

For more information, see the following topics:

"Starting zSecure programs using JCL" on page 690
"Starting zSecure through line mode commands" on page 696
"IBM Security zSecure JCL procedures" on page 696
"IBM Security zSecure jobs" on page 699
"Using the scripts in the IBM Security zSecure CARLa library" on page 706

Starting zSecure programs using JCL

Table 279 provides an overview of IBM Security zSecure programs that can be called using batch jobs. Each program provides a link for additional information about JCL that can be used to call the program.

Table 279. Calling IBM Security zSecure programs using batch jobs

Program	Description	Details on calling through JCL
CKRCARLA CKRCARLX (used when APF authorization is required)	Uses the special purpose Auditing and Reporting language (CARLa) to process RACF SMF, Access Monitor, and other types of information. The program is used by the following zSecure products: Admin, Audit, Alert, Visual, and the Compliance Insight Enabler for z/OS.	"CKRCARLA and CKRCARLX" on page 691
CKGRACF	Used for handling Queued commands (like temporary access), revoke or resume schedules, User data fields and various other functions that require updating RACF profiles. This program is used by zSecure Admin and zSecure Visual.	"CKGRACF" on page 693
CKNSERVE	The main program for the zSecure Server that performs the necessary functions for communicating with remote systems to route commands and access RACF databases, SMF input files, CKFREEZE data sets, and other defined data sets.	For more information on the zSecure Server, see the "Using remote data" on page 4 and the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.
CKX (Command Execution Utility)	CKX is the IBM Security zSecure Command Execution Utility that issues TSO commands. Contrary to directly executing the commands with IKJEFT01	"CKX - Command Execution Utility" on page 693
C2PACMON (Access Monitor)zSecure Admin	Collects information about RACF usage data that can be used to remove unused or obsolete resource profiles or test usage scenarios. This program is supported by zSecure Admin.	*IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*

Table 279. Calling IBM Security zSecure programs using batch jobs (continued)

Program	Description	Details on calling through JCL
C2XACTV (RACF Exit Activator)	Provides dynamic exit support for some RACF exits. This script installs the exits required by various zSecure products including zSecure Admin, Audit, Alert, and IBM Tivoli Compliance Insight Manager Enabler for z/OS.	"C2XACTV - RACF Exit Activator" on page 693
CKFCOLL (zSecure Collect)	The zSecure Collect program, CKFCOLL gathers information about your z/OS system configuration. The program is designed to collect data quickly using minimal system resources. The data collected is analyzed by the CKRCARLA program.	"Configuring zSecure Collect" on page 1594
RACF Offline	Function for running and testing RACF commands on a RACF database that is not active in the system. This function is available in zSecure Admin.	"Activating" on page 596

CKRCARLA and CKRCARLX

CKRCARLA, the main program of zSecure Admin and Audit, performs the following functions:

- Interprets the CARLa code.
- Collects data from the security database, CKRFREEZE files, SMF, and other data.
- Generates reports based on the data collected.

Typically, CKRCARLA runs without APF authorization. If APF authorization is required, you can use the front-end program CKRCARLX. Using CKRCARLA with APF requires READ access to resource CKR.CKRCARLA.APF. For details, see *Appendix B: zSecure-specific security resources* in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Chapter 12, "CARLa Command Language," on page 713 describes which functions require APF authorization. Running with APF authorization affects any Writer to Operator (WTO) messages that might be issued: For programs without APF authorization, the system prefixes all WTO messages with a +. As a result, your message automation might be impacted when operation switches between programs running with APF authorization and programs running without it. To prevent message spoofing, CKRCARLA prefixes a + to any message that does not start with C2P1 through C2P8 when running with APF authorization. The changes can also disturb alignment in a multiline WTO message.

To call the IBM Security zSecure main program in batch mode, use the IBM Security zSecure cataloged procedure C2RC, for example:

```
// JCLLIB ORDER=(MY.CKRPARM,CKR.SCKRPROC)
//  EXEC  C2RC,ALLOCCKF=1,CONFIG=MYCONFIG
//SYSIN   DD *
  n type=system
  sortlist  sysname esmname esmlevel
```

If the zSecure procedures and configuration file are configured for your system and available in a standard procedure library, you can leave out the JCLLIB statement. Check with your system administrator for information.

For information about the zSecure cataloged procedures, see "IBM Security zSecure JCL procedures" on page 696.

For more control over file allocation, you can start CKRCARLA using the following code:

```
 //   INCLUDE  MEMBER=MYCONFIG
 //ZSECURE EXEC PGM=CKRCARLA,REGION=128M,
//    PARM='ALLOCATE INDD=CARLA OUTDD=REPORT'
//STEPLIB  DD DISP=SHR,DSN=&CPREFIX..SCKRLOAD
//REPORT   DD SYSOUT=*
//CARLA    DD *
 <subsequent CARLa>
```

In this example, the PARM field contains the first CARLa command. You can specify multiple commands separated by a semicolon.

This ALLOCATE statement reads the commands from the ddname CARLA instead of using the default SYSIN. Reports and messages are redirected to the ddname REPORT instead of using the default SYSPRINT. Because of this redirection, the CKRCARLA program does not need any fixed ddnames, except for STEPLIB. For information about the CARLa syntax, the ALLOCATE command, and how to redirect other DD statements, see Chapter 12, "CARLa Command Language," on page 713.

You can concatenate data sets with like attributes for all input ddnames. However, do not concatenate data sets that contain CKFREEZE or UNLOAD files. DD-statements used to specify these input files only require a single file, so concatenation is not necessary.

Two-pass queries

For two-pass CARLa queries the procedure C2RC2 is available. See "IBM Security zSecure JCL procedures" on page 696. C2RC2 is a nested JCL procedure, the procedure uses another procedure C2RC to do its work. There is a restriction in z/OS Job Control Language on overriding statements in nested procedures. Overriding is restricted by so many rules that in practice it is impossible. You can use the procedure C2RC two times to do the same.

A partial example of JCL for a two-pass query:

```
//* generate CARLa statements to be used in pass 2
//STEP1    EXEC C2RC,CONFIG=&CONFIG.
//CKR2PASS DD DISP=(NEW,PASS),UNIT=SYSDA,SPACE=(255,(2000,2000))
//    DSN=&&PASS1
//SYSIN DD *
  option dd=ckr2pass nopage
  newlist type=racf outlim=1
    sortlist  "report scope=(,"

  newlist type=racf
    s c=user s=base operations
    sortlist  key(8) ","

  newlist type=racf outlim=1
```

```
    sortlist  ")"
/*
//* Execute the CARLa generated by STEP1
//STEP2    EXEC C2RC,CONFIG=&CONFIG.
//SYSIN DD DISP=(OLD,PASS),DSN=&&PASS1
```

CKGRACF

A typical way to start CKGRACF is:

```
//   INCLUDE  MEMBER=MYCONFIG
//CKGRACF  EXEC PGM=CKGRACF,REGION=6M,PARM='INCLUDE DDNAME=CKGIN'
//STEPLIB  DD DISP=SHR,DSN=&CPREFIX..SCKRLOAD
//CKGPRINT DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//CKGIN    DD *
 <subsequent CKGRACF commands>
```

The INCLUDE statement in the PARM field is necessary to process an input ddname.

Without redirection, you can use the ddnames listed in "Supported file definitions for CKRCARLA" on page 701.

CKX - Command Execution Utility

CKX is the IBM Security zSecure Command Execution Utility that issues TSO commands. This utility differs from the IKJEFT01 utility for directly executing commands in the following ways:

- CKX returns a nonzero return code if any command had a nonzero returncode. not just the last one like IKJEFT01 only returns a nonzero return code if the last command has one.
- At the bottom of the CKXDEBUG file, CKX summarizes command failures for reviewing. IKJEFT01 does not provide a summary which makes it more difficult to note all the failed commands, especially when hundreds or thousands of commands are run.

You can start CKX using the following code:

```
//   INCLUDE  MEMBER=MYCONFIG
//CKX     EXEC PGM=IKJEFT01,REGION=64M,PARM='CKX DD=CKX@IN'
//STEPLIB  DD DISP=SHR,DSN=&CPREFIX..SCKRLOAD
//CKXDEBUG DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//SYSTSIN  DD DUMMY
//CKX@IN   DD *
 <CKX commands here>
```

Optionally, you can allocate the file CKXT@PRT. This file contains the data created by TSO commands called from the product. The default settings for following DCB parameters are: LRECL=255 and RECFM=VB. Line length is 251, except when sending data to a z/OS UNIX path. For UNIX system, the line length is 32752. Block size defaults to half track if a full track is larger than 32 KB.

C2XACTV - RACF Exit Activator

The RACF Exit Activator program, C2XACTV provides dynamic exit support for some RACF exits. The RACF Exit Activator program is designed primarily for installing the exits required by various zSecure products.

The RACF Exit Activator program offers support for RACF pre-, main-, and post-exits. If you already have RACF exit routines in place, the program uses these routines as sub exits. Before using the zSecure exits, confirm that the exit routines can coexist with the RACF exit routines.

In most cases, you do not need to control the exit explicitly:

- The C2XEXITS parameter controls the ICHPWX01 exit. This parameter is specified in the zSecure configuration files used by zSecure Alert and the Tivoli Compliance Insight Manager Enabler for z/OS.
- The other exits are automatically activated or deactivated when the Access Monitor program is started and stopped.

You must activate exit ICHPWX01 explicitly if you are using zSecure Audit by itself. In this case, activate the exit to process the additional SMF records that ICHPWX01 generates for all password change events. You can also activate the exit to apply maintenance changes to a module without having to IPL the system. Activation explicitly refreshes the exit.

The following table summarizes the supported exits and associated functions.

Table 280. Exits supported by the C2XACTV program

Exit	Function
ICHPWX01	ICHPWX01 is the RACF New Password exit that logs all password change events. This exit is included in zSecure to complement the RACF-generated, new password SMF records. For z/OS release 1.6 and earlier, RACF only logs password changes through the ALTUSER and PASSWORD commands. With the ICHPWX01 exit, RACF also logs password changes that occur through logon or signon events or through a JOB-statement in JCL. Use the ICHPWX01 exit to track all password changes during audit processing. zSecure Alert and Tivoli Compliance Insight Manager Enabler for z/OS use this exit. Typically, the C2XEXITS parameter controls the exit. The ICHPWX01 exit only writes an SMF record and does not change control blocks. However, if you have your own exit that does change control blocks. the changes might affect the contents of the SMF record.
ICHRDX02, ICHRCX02, ICHRFX04	RACF calls these exits in the following situations: • When the program runs AUTH or FASTAUTH commands during access verification. • When the program runs DEFINE commands during the process to create, update, or delete data sets and resource profiles. The Access Monitor program also uses these exits, automatically activating and deactivating them as needed. These exits do not affect regular processing; do not update control blocks, and do not add or modify SMF records.

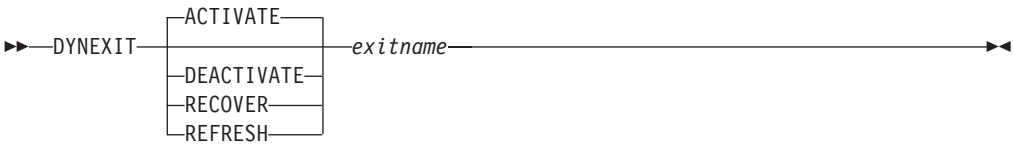
Use the following code sample to run the Exit Activator:

```
// JCLLIB ORDER=(MY.CKRPARM,CKR.SCKRPROC)
//  EXEC  C2RCACTV,CONFIG=MYCONFIG,PARM='DYNEXIT ACTIVATE ICHPWX01'
```

The zSecure RACF Exit Activator requires at least one of the following products: zSecure Admin, zSecure Audit for RACF, zSecure Alert for RACF or Tivoli Compliance Insight Manager Enabler for z/OS. zSecure Alert and Tivoli

Compliance Insight Manager Enabler for z/OS automatically establish the New Password exit automatically. However, you can run the DEACTIVATE command to turn it off.

The report data from the exit goes to the C2XPRINT DD statement. You can supply the commands for the RACF Exit Activator either on the PARM field or through a C2XIN DD statement. The RACF Exit Activator has the following syntax:



The following list describes the commands and parameters:

ACTIVATE turns on the RACF exit. If the currently installed exit is the one provided by the RACF Exit Activator program C2XACTV, the program issues an error message and stops.

The ACTIVATE command loads the Dynamic Exit Support routine and changes the RCVT pointer so that the routine is called by RACF. If another exit routine exists before C2XACTV runs, that exit routine is started as a Functional Exit Routine of C2X.ICHPWX01. If the RCVT pointer is zero–indicating that no exit point is in use–an exit point for C2X.ICHPWX01 is defined, but no Functional Exit Routine is installed.

exitname identifies the exit point you want to activate, deactivate, recover, or refresh. See Table 280 on page 694 for a list of supported exit points.

DEACTIVATE turns off the exit. If the ACTIVATE function replaced an existing RACF exit module, the original RACF exit module is reinstated during the deactivation process.

RECOVER removes the dynamically loaded exit routines from storage and restores the system to its previous state. You can only issue this command after the corresponding dynamic exit is de-activated. Use this command with extreme care. Programs that load the address for a RACF exit routine without checking whether the address is still valid might experience various abends after running the RECOVER command.

In most situations, you do not need the RECOVER command. Because the modules loaded into LPA by the C2XACTV program are typically less than 4K in size, removal is hardly ever required.

REFRESH determines whether the specified exitpoint is installed. If it is, zSecure refreshes all modules from the same source specified during the activation process. If the exitpoint is unavailable, zSecure creates an error message and exits the program. Existing Functional Exit Routines for C2X.ICHPWX01 might not be changed.

Additional exit routines are defined for pre- and post-processing Functional Exit Routine. These routines are independent of the REFRESH or ACTIVATE function, The exit routines provided by the C2XACTV program are loaded and linked to these pre- and post-processing exits.

For additional information about the RACF Exit Activator, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Starting zSecure through line mode commands

To start programs from line mode, replace all DD statements except JOBLIB and STEPLIB with ALLOCATE commands (TSO) . You can start the program by typing the program name or program path (z/OS UNIX). You can specify the command manually or using a script. The ISPF interface is such a script.

CKRCARLA

You can start CKRCARLA directly from TSO, with semicolon-separated CARLa commands as parameters.

In addition, the version of CKR supplied with IBM Security zSecure accepts MODE(LINE) on its input. Your installer might have established installation-specific copies of CKR, perhaps under different names. For information, consult your installer. Use the default CKR program or installation-specific copies of this program to run the product in line mode.

If your site has a previously prepared data set member that contains your CARLa statements, use the following commands to run the commands in line mode:

```
ALLOC FILE(SYSIN) SHR REUSE DA('MY.CARLA(MEMBER1)')
%CKR MODE(LINE)
```

Note: You cannot supply line mode input from a terminal or use ALLOC FILE(SYSIN) DA(*). To process terminal input, do the following:

1. Create a script to generate the CARLa commands based on the terminal input data.
2. Write the CARLa commands to a data set.
3. Start the program and use the data set created in Step 2 to run the commands.

CKGRACF

In addition to the TSO CALL method, you can also call CKGRACF in line mode: Type the following CKGRACF command directly after the program name at the TSO READY prompt:

```
CKGRACF RDELETE FACILITY '*' DISCRETE
```

The CKGRACF program is only supported by zSecure Admin.

IBM Security zSecure JCL procedures

IBM Security zSecure provides a number of JCL procedures that can be customized for use in your environment. See the following topics for details:

- "C2RC and the naming convention for your data sets"
- "Other zSecure procedures" on page 697

C2RC and the naming convention for your data sets

The general purpose JCL procedure C2RC can be used to run the main zSecure program with the specified CARLa member from the SCKRCARL library. You can override the SYSIN DD-statement if your CARLa member is stored in another library. You can also use instream (DD * or DD DATA) CARLa statements. The C2RC procedure provides the following parameters:

MEMBER=
Specifies the pre-defined member to run.

ALLOCSMF=*n*
Determines whether to allocate SMF (`ALLOCSMF=1`) or run without allocating SMF (`ALLOCSMF=0`).

ALLOCCKF=*n*
Determines whether to allocate a `CKFREEZE` data set (`ALLOCCKF=1`) or run without allocating one (`ALLOCCKF=0`).

ALLOCUNL=*n*
Determines whether to allocate an UNLOAD data set (`ALLOCUNL=1`) or use the live RACF database (`ALLOCUNL=0`).

CKRCMD=*n*
Specifies the action for the file. Use 1 to allocate `CKRCMD`, 0 for `SYSOUT=*`.

DSTAT=OLD
Specifies the disposition for the `CKRCMD` file.

OPTCARLA=
Specifies any additional CARLa statements or settings.

This procedure, and several others, use several `INCLUDE`-members. To create the procedure, specify values for the following parameters: `ALLOCSMF`, `ALLOCCKF`, `ALLOCUNL`, and `CKRCMD`. These `INCLUDE`-members represent a naming convention for your `SMF`, `CKFREEZE`, `UNLOAD`, and `CKRCMD` data sets. If your naming conventions do not match the conventions in the shipped C2RI* members, create your own members with these names in a data set of your own. For example, create members in the data set where you store the configuration members and point to that data set with a `JCLLIB` statement. Possibly, your installer has created customized members in a standard procedure library on your system.

Other zSecure procedures

zSecure provides other JCL procedures for specialized tasks. Several of these procedures call the `C2RC` procedure. Due to a z/OS restriction, you cannot add or override DD statements on the `C2RC` job step when you start the outer procedure. If you must run any DD statement additions or overrides, call `C2RC` directly. For an example, see "Two-pass queries" on page 692.

Note: Your product data sets might not contain all the members documented in this topic. The members included depend on which products and product options are installed on the system.

The following procedures are provided with zSecure:

CKACTM, CKACTPRT, CKACTSRT, CKACTSYS
These procedures apply to the Change Tracking system. For details, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2EAUDIT, C2ECLSMF, C2ECSTOP
These procedures apply to the Agent for Tivoli Compliance Insight Manager Enabler for z/OS. For information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2PACMON
Manages the Access Monitor function available in IBM Security zSecure Admin. The Access Monitor collects usage data on resource profiles and the authorizations defined within the profile. The data can be used to identify

unused or obsolete profiles and access permissions so they can be corrected or removed. For information about setting up the C2PACMON program, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. For information about using it, see Chapter 10, "RACF Access Monitor," on page 643.

C2PCOLL, C2PCRECI, C2POLICE
These procedures apply to zSecure Alert. See the zSecure Alert User Reference Manual.

C2RCACTV
This procedure establishes the IBM Security zSecure RACF Exit Activator. For additional information, see the topic"Starting zSecure programs using JCL" on page 690 and the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2RCMSYN
For zSecure Admin, this synchronizes two RACF databases using merge. You must supply data set names for the two input parameters: `CORRECT` and `ONE2FIX`. These parameters represent two `UNLOAD` files. The program updates all profiles in ONE2FIX data set so they match the equivalent profiles in the CORRECT data set. The program uses a standard MERGE command to generate the RACF commands for adding missing profiles and updating existing ones. You run a separate process to generate the RACF commands to delete profiles from the ONE2FIX file that are not present in CORRECT file.

C2RCXCKG
Runs CKGRACF commands. Supply the commands through a `CKGIN` DD-statement.

C2RCXTSO
Runs RACF and CKGRACF commands that have been generated by IBM Security zSecure. For input, specify a data set that has been created by a previous job or step that runs procedure C2RC with `CKRCMD=1`. If your input comes from another location, override the `SYSTSIN` DD-statement.

C2RC2
A general two-phase CARLa procedure: The first job step writes the CARLa code to the DD-statement `CKR2PASS`. The second job step runs the code in the first job step. You can specify the following parameters:

MEMBER=
Specifies an existing member that includes the code to run.

ALLOCCKF=0
Determines whether to allocate a `CKFREEZE` file. Specify one `1` allocate the file. Specify `0` to run without allocating it.

ALLOCUNL=0
Determines whether to allocate an `UNLOAD` file for RACF. Specify one `1` allocate the file. Specify `0` for the live database.

CKRCMD=0
Determines whether to allocate a `CKRCMD` file. Specify one `1` allocate the file. Specify `0` to use SYSOUT=*.

OPTCARLA=
Specifies any additional CARLa statements to run.

C2RSERVE, C2RSLOG, C2RSTOP
These procedures are used with IBM Security zSecure Visual. See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

IBM Security zSecure jobs

The SCKRSAMP data set in the product supplies a number of sample jobs. Before using the jobs, you must update the data set names and other parameter variables for your environment. For example, you must update jobs that include a print step to add the correct print destinations. Before you customize the jobs, copy them to your own data set. You need the original versions of the jobs in the SCKRSAMP library so that you can copy and customize them for use in different zSecure configurations. In addition, if the modified jobs are saved in the SCKRSAMP library future maintenance or upgrades might overwrite your customization because the SCKRSAMP library is SMP/E managed.

A partly customized copy of the SCKRSAMP library known as the CKRINST library is normally created during the installation process. For details, see *Installing the software* in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. If you deploy zSecure on multiple z/OS images, you might require more than one copy of the customized SCKRSAMP library for the different images.

Before using these jobs, customize them for your z/OS image and the specific department or organization that the job supports. Copy the job, and then update the data set names and parameter values. Specifically, check the jobs to determine whether they require any of the following updates:

- Most of the zSecure jobs contain a JCLLIB statement that specifies your configuration data set and the SCKRPROC data set. Verify that the data set names are the correct ones for your installation. Typically, the referenced data sets have been renamed or copied to a standard procedure library for your JES. For example, the configuration data set name is always unique to your organization.
- Many jobs also pass a specific zSecure configuration file name when calling a procedure. Make sure that the job specifies the correct configuration file for the context where the job is used.

The following list describes the zSecure sample jobs. Your product data sets might not contain all the members listed. The members included depend on which products and product options are installed on the system.

CKAJTCT1, CKAJTCT2, CKAJTCT3, CKAJTM, CKAJTSRT, CKAJTSYS
These jobs apply to the Change Tracking system. For additional information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2AJFMBV
This procedure applies only to zSecure Audit for ACF2. The RACF version of this job is C2RJFMBV.

C2EJSTOP, C2EJSTRT
These procedures apply to the Tivoli Compliance Insight Manager Enabler for z/OS for the Tivoli Compliance Insight Manager or Tivoli Security Information and Event Manager. For details, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2PJRECI
This job applies only to zSecure Alert. See the *IBM Security zSecure Alert: User Reference Manual*.

C2RJ
Generates a collection of standard reports. To generate reports, uncomment the statements for the reports you need. See procedure C2RC for parameters.

C2RJFMBV
Report on violations per department through email. The following statements and parameters need site-specific customization:

OPTCARLA=option emt=*POSTMASTER@C2RCUSTD* Specify the email address of the person to receive the report bundles that did not get an email address through the EMAIL lookup data set. This address is also used for the email sender, but not for the reply-to address. The option parameter EMT is the abbreviation for ERRORMAILTO.

SMTPNODE= Specify the NJE node where SMTP runs with parameter.

SMTPOUT=B Change this value to the SYSOUT class for SMTP output.

EMAIL DD Change the inline ddname contents to contain the correct addresses

C2RJFUNL
Unloads and selects SMF records from live SMF data.

- You can customize this job to specify the SMF record types to be collected in the inline SYSIN data set.
- Add the specific number of your HSM functional statistics record rather than only specifying SETSYS SMF.
- Confirm that the /*JOBPARM S= and SYS= parameters specify the same system.

Note: If the first character of the system name is numeric, you must add an alphabetic character to the SYS= parameter to prevent invalid data set names.

C2RJMALL
Merges the profiles in an UNLOAD of a remote database into the current database. For details, see the Chapter 9, “Merge Usage Guide,” on page 623. Update the ALLOC statements before submitting the job.

C2RJMDIF
Merges the profiles from the active backup database into another database so it matches the live database. If merge conflicts occur, the profile data from the active backup database takes precedence. The output in CKRCMD consists of the commands to merge the profiles. For details, see the Chapter 9, “Merge Usage Guide,” on page 623. Be sure to adapt the ALLOC statements before submitting the job.

C2RJMGRP
This job shows how to merge group A into group B. In the job, the same database is used as source and as current database. Before using the job, make the following changes:

1. Adapt the ALLOC statements to suitable UNLOAD files.
2. Replace the occurrences of *A* and *B* on the X and MERGERULE statements by the names of the groups you want to merge.

C2RJMSYN
This job synchronizes two RACF databases using merge. Before using the job, review the following items and make any required changes:

Notes:

1. This job expects two UNLOAD files as input.
2. To use a database copy, Change the ALLOC statements for the various SYSIN files. You do not need to edit the PROC statement.
3. If you must run the job multiple times to complete the synchronization the process, change the DISP value for the output data sets on subsequent runs.

4. By default, the job sends all generated RACF commands to the same CKRCMD file. To send the commands to delete profiles to a different CKRCMD file, uncomment the DD statement at the bottom of the job and change the parameter values.

C2RJPREP
Create or refresh a CKFREEZE file, an UNLOAD file, or both. For more information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2RJRSYN
Generates RACF commands to synchronize the RACF database with actual data sets present on a single volume. Specify the volume in the job.

C2RJSERV
This job applies to the zSecure Visual product. See the zSecure Visual Server Manual.

C2RJXCKG
See procedure C2RCXCKG.

C2RJXRFR
This CKGRACF daily job applies only toIBM Security zSecure Admin. See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2RJXSAS
This job performs a pre-defined function on previously unloaded data to generate input for post-processing with SAS.

C2RJXTSO
See procedure C2RCXTSO.

C2RJ2
Generates a collection of reports requiring two-pass CARLa. To generate reports, uncomment the statements for the reports you need.

Supported file definitions for CKRCARLA

If redirection is not used, the following file definitions (FILEDEFs) are supported by the CKRCARLA program.

STEPLIB
STEPLIB or JOBLIB identifies the library containing the installed program.

SYSPRINT
Indicates the destination for listings and messages. This file type might require changing the settings to accommodate longer text lines (LRECL) and different record formats (RECFM).

LRECL The default logical record length does not support longer line lengths. The default relies on other DCB parameters to extend the text length to 132 when necessary. To support longer line lengths explicitly, change the default LRECL setting to a higher value. The maximum supported value is 32760.

RECFM (record format) supports the following values:

- **F** for fixed format
- **FB** for fixed-length, blocked
- **VB** for variable, blocked
- **FA** for fixed-length, ASA carriage-control characters
- **VA** for variable, ASA print-control characters

- **FBA** fixed, blocked, with ANSI carriage control characters
- **V** for variable format
- **VB** for variable, blocked
- **VBA** variable, blocked, with ANSI carriage control characters
- Record Format

The default record format is VBA. For 3800-type laser printers, you can add the OPTCD=J parameter to the DCB parameters in combination with the CHARS=(norm,bold) parameter. The value norm specifies the character set for normal text; bold specifies the character set for bold text.

The default block size is approximately half track if a full track is larger than 32 KB, and consistent with the LRECL and RECFM values.

SYSIN
File type for specifying the CARLa command input. For command documentation, see Chapter 12, "CARLa Command Language," on page 713. This file type supports a maximum LRECL of *32760* and supports both the RECFM=F(B) and RECFM=V(B) format settings.

SYSTERM
The SYSTERM file is an optional file that you can allocate to receive messages. This file receives messages issued in response to a return code of 12 or higher and a number of status messages. Issue one of the following commands to receive the messages on the screen:

- Under CMS, issue the following command: FILEDEF SYSTERM TERMINAL.
- Under TSO, issue the following command: ALLOC F(SYSTERM) DA(*).

CKRCARLA
The CARLa IMBED or INCLUDE statement use this ddname if the MEMBER was specified without a value for DDNAME.

C2REMAIL
Determines the destination of the following email commands: MAILTO and BUNDLEMAILTO. If you have not allocated this file, the SMTP (Simple Mail Transfer Protocol) settings are used to route email.

You can specify the email settings using the following keywords on the OPTION command SMTPWRITER, SMTPCLASS, and SMTPNJENODE. If you do not specify any keywords, the default values are in effect.

Use the following statement to allocate the C2REMAIL file directly to the email server:

```
SYSOUT=(outputclass,SMTP),DEST=&SMTPNODE
```

&SMTPNODE is the name of the JES2 or JES3 or RSCS node where SMTP is active.

SMTP is the writer-name of the installed SMTP. This value defaults to SMTP. However, the value might be different, depending on the installation path.

You can specify an LRECL value of 255 or higher. To support EBCDIC to HTML translation, specify an LRECL value that is 796 or higher. This value increases the line length up to six times the length of the original default length (132). Do not use RECFM=VBA or RECFM=VBM because they are not supported by all SMTP writers.

Alternatively, you can allocate this file to a data set to analyze the emails rather than sending them. You can reach the same result by allocating a C2RSMTP DD, and using the SMTPTOFILE command.

Note: The email function of Security zSecure is not intended to be used with the INFOPRINT email support introduced in z/OS V1R5.

C2RSMTP
File that receives redirected email when the SMTPTOFILE command is used. To support EBCDIC to HTML translation, specify an LRECL value that is 796 or higher. This value increases the line length up to six times the length of the original default length (132). Do not use RECFM=VBA or RECFM=VBM because they are not supported by all SMTP writers.

Use the following fields to build an email:

HELO
Required. Specifies an RFC2821 domain name. Make sure that reverse lookup of this name returns the sending IP address, otherwise mail might be refused. The domain name comes from the local host name returned by the TCP/IP stack GETHOSTNAME or GETHOSTBYNAME command. If this command fails, the program checks the following parameters in the order listed to obtain the first available domain name: SMTPMAILFROM, ERRORMAILTO, FROM, or REPLYTO.

RCPT TO
Required. Specifies an RFC2821 address for SMTP mail delivery. The value is constructed from the fields MAILTO, CC, and BCC.

MAIL FROM
Required. Specifies an RFC2821 address for SMTP routing of non-deliverable message notifications. The program determines the value by checking the following fields in the order listed and uses the first available address: SMTPMAILFROM, ERRORMAILTO, REPLYTO, or FROM.

From
Required. Specifies an RFC2822 address. The program determines the value by checking the following fields in the order listed and uses the first available address: FROM, SMTPMAILFROM, ERRORMAILTO, REPLYTO.

To
Generated field. Specifies an RFC2822 address. It is constructed from the MAILTO field.

CC
Optional. Specifies an RFC2822 address. It is constructed from the CC field.

BCC
An RFC2822 address. It is constructed from BCC. This field is optional.

C2RSNMP
File that receives the redirected output from SNMP when the SNMPTOFILE command is used. To support the line length for writing SNMP traps, specify the following values for the record format and line length: RECFM=VB,LRECL=1060

C2RSYSLG
File that receives the redirected output from the UNIX syslog when the OPTION SYSLOGTOFILE setting is specified. To support the line length for writing syslog traps, specify the following values for the record format and line length: RECFM=VB,LRECL=2048.

C2RWTO
File that receives the redirected output from the Writer to Operator (WTO) function when the WTOTOFILE command is issued.

CKRCMD
Optionally, you can allocate the CKRCMD file (implicit allocation mode only). This file receives the command output generated as result of COPY, MOVE, REMOVE, or VERIFY operations. Allocating the file implies that TSO commands must be generated where possible.

The default values for data control block (DCB) parameters are as follows:

LRECL
The default logical record length depends on the CKRCARLA execution environment. For batch jobs, the default record length is 255 bytes. For new users, the ISPF user interface allocates data sets with default settings of RECFM=FB and LRECL=80. To change the RECFM and LRECL settings, see "SE.0 Setup - Run Options" on page 1643. When sending output to a z/OS UNIX file, the default line length is 32752 bytes whether you execute CARLa commands as a batch job or run commands from the ISPF user interface.

RECFM

The default record format depends on the CKRCARLA execution environment. For batch jobs, the record format is variable length (VB). For new users, the ISPF user interface allocates data sets with a record format of fixed length (FB) as the default. To change the RECFM setting in the run options, see "SE.0 Setup - Run Options" on page 1643.

For VB records, the first 8 bytes of each line are blank because TSO EXEC program processing expects line numbers in these positions and ignores them. For fixed length (FB) records, the last 8 bytes are blank unless you have specified an overriding line length by using LL=*value*.

Block size

The block size defaults to half track if a full track is larger than 32 KB.You can run CKRCMD as a CLIST or pass the file to the Command Execution Utility (CKX).

For security reasons, make sure that erase-on-scratch is in effect for this data set.

CKRUNLOU
Unloads data from the specified data input sources. This optional file is used for UNLOAD operations.

If you are using IBM Security zSecure Admin, the UNLOAD operation is requested automatically when allocating the file.

CKRUNLIN
In implicit allocation mode, you have the option to allocate this file. If allocated, change the CKRUNLIN parameters to point to a file with a previously unloaded security database. No records are read from the current security database. See the comment on CKRUNLOU.

CKRACF01
Optionally, you can allocate this file to indicate where the RACF master data set or its backup copy can be found–only in implicit allocation mode. If you omit CKRACF01 and CKRUNLIN, the currently active primary RACF master data set is allocated dynamically along with other primary data sets for CKRACF*nn*.

CKRACFnn
If you allocate CKRACF01, you can also allocate CKRACF02 and up to indicate additional non-master RACF data sets or their backup or archive copies. If you omit CKRACF01 and the RACF database has more than one data set, the remaining currently active primary data sets or whatever else has been implied by an ALLOC command are automatically allocated.

SYSTCPD
This DD-statement might be necessary when you write reports in SMTP- or SNMP-format. This type of reporting requires TCP/IP communication and possibly, translation of domain names into IP addresses and reverse. Your IP-stack might have other ways to provide for this translation. Consult the IP configuration documentation for your system.

CKFREEZE
Optional. You can allocate this file to receive information about the following types of data gathered from the system using zSecure Collect (implicit allocation mode only): `VTOC`, `VVDS`, catalogs, `HSM` data, `DMS` data, `CA1` data, `PDS` directories, `UNIX` file system content, and so on.

The `CKFREEZE` file, or `CKRCKF0`*n*) is required for the following command processing:

- `VERIFY` options: `ONVOLUME`, `INDICATED`, `NONEMPTY`, `PROGRAM`, and `PGMEXIST`
- `REPORT` options: `DATASETS`, `AC1`, and `PADS`.

CKRCKF0-n
Optionally, you can allocate the files CKRCKF00 - CKRCKF09 instead of or in addition to the CKFREEZE file. Use these files to provide collected configuration data from multiple systems (implicit allocation mode only).

CKREPORT
If allocated, this file automatically receives the data from the `REPORT` command unless the `REPORT` command is preceded by an `OPTION` or `PRINT` command with a specified `DDNAME=`. In this situation, the data is written to the specified ddname rather than the `CKREPORT` file. For default settings, see `SYSPRINT`.

CKRSMFnn
Optionally, you can allocate the files `CKRSMF00 - CKRSMF99` instead of or in addition to SMF. Use these files to provide additional SMF input (implicit allocation mode only). Not used with IBM Security zSecure Admin.

<any input dd>
Specifies any ddname that is specified in an `INCLUDE` or `IMBED` statement.

<any output dd>
Specifies any ddname that is specified in the `DDNAME` parameter for the `OPTION` or `FILEOPTION` commands. Any `LRECL` and `RECFM` specifications on the JCL DD statement are honored. For a list of supported values and other considerations, see the SYSPRINT file definition.

If you do not specify values for `LRECL` or `RECFM`, zSecure determines them based on the type of data directed to the ddname. For `LRECL`, zSecure uses the largest effective `LINELENGTH` for any `NEWLIST` command directed to the output file. The program also considers other DCB parameters for writing lines of this length. The `LRECL` selected matches one of the following:

- An explicit `LINELENGTH` parameter for this ddname on one of the following statements or commands: `OPTION`, `FILEOPTION`, `BUNDLE`, or `NEWLIST`.
- The default `LINELENGTH`, which is 132 for a data set and 32752 for a UNIX file.

By default the record format (RECFM) of a data set is VBA. This default is only changed to VB if all NEWLIST commands for this ddname have specified NOPAGE directly on the NEWLIST statement or through one of the following commands: OPTION, BUNDLE or FILEOPTION.

CKR2PASS
This file is only written through the DDNAME parameter, as documented on the OPTION command. It has the same default characteristics as CKRCMD. It is intended for two-pass CARLa, as in the procedure C2RC2 and in the ISPF interface.

Using the scripts in the IBM Security zSecure CARLa library

Several CARLa scripts are supplied in the SCKRSAMP library. Most of these scripts are used by the ISPF interface and by IBM Security zSecure jobs and JCL-procedures.

Note: Your product data sets might not contain all the members documented in this topic. The members included depend on which products and product options are installed on the system.

Naming convention

As a first classification, the first three characters indicate the component or feature for which the script is intended:

Table 281. Product prefixes for CARLa scripts

Prefix	Component or feature
CKA	zSecure Audit for RACF
CKG	CKGRACF component IBM Security zSecure Admin
CKR	IBM Security zSecure Admin
C2A	zSecure Audit for ACF2
C2E	Tivoli Compliance Insight Manager Enabler for z/OS
C2P	zSecure Alert
C2R	zSecure Visual or zSecure Admin and Audit common
C2X	zSecure RACF Exit Activator

The fourth character represents the type of the script:

Table 282. Character indicating type of CARLa script

Type code	Use
D	Interactive display queries (some can also be used to produce batch reports).
L	Batch reports (not intended for interactive use).
R	Default layouts for CARLa REPORT commands (backwards compatibility)
S	Inclusion members with CARLa DEFINE statements for SMF or other logs
V	Verify commands.
X	Used from the Security zSecure ISPF interface.

Customizable CARLa scripts

Some CARLa scripts specify items like data sets and RACF groups with names that do not match the names in installation. You can customize these scripts to specify the correct names. However, do not customize the original members in the SCKRCARL data set. Because this library is managed by SMP/E, future maintenance might overwrite your customization. In addition, changing members within the shipped SCKRCARL data set would violate distributed-oriented installation conventions. To customize the scripts, create copies in a data set of your own, and use this data set concatenated in front of the shipped CARLa library.

For an individual user, you can specify the use of this local data set in the UPREFIX parameter in the IBM Security zSecure configuration. For a group of users the WPREFIX parameter is more appropriate. UPREFIX and WPREFIX are described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Table 283 lists the CARLa scripts that you can customize.

Table 283. CARLa customizable scripts

Script	Customization
CKALFJOB	You might want to add a select statement to the SMFSEL NEWLIST to select specific users and then uncomment the NEWLIST. Alternatively, you can include the CARLa script after an earlier NEWLIST named SMFSEL.

CKRDPWIN
CKRLPWIN
	Creates reports that show user IDs that do not change their passwords often because they have an exceptionally long password interval. The interval can be long because the user profile has one of the following conditions:
	• An exceptionally long password interval
	• No password interval.
	• Can logon without a password.
	• Can log in with an OIDCARD.
	When you configure the report, you can customize the length of the password interval for selecting records by editing the PWINLONG NEWLIST. To keep the report manageable, exclude started task user IDs from these reports. If you have a special purpose group that your started task user IDs are connected to, you can exclude the name for the started task user group (stcgroup) in the select statements for PWINLONG and PWINNONE.
	Here is the select statement for PWINLONG:
	`select class=user`
	`segment=base`
	`passint>60 passint<255,`
	`congrpnm<>stcgroup`
	`/* exclude started tasks */`
	If you consider *exceptionally long* to be more than 30 and your started tasks are connected to a special STRTASK group, customize this statement as shown in the following example:
	`select class=user segment=base passint>30`
	`passint<255,`
	`congrpnm<>strtask /* exclude started tasks */`

CKRDPWNU CKRLPWNU CKRDLGNU CKRLLGNU	Specify the correct connect group name (congrpnm) to recognize started tasks in the WHERE clause of the DEFINE STCGROUP statement. The default group name is STCGROUP.

Table 283. CARLa customizable scripts (continued)

Script	Customization
CKRDPWXP CKRLPWXP	You must specify the correct connect group name (`congrpnm`) to recognize started tasks by in the select statement. The default is `STCGROUP`.
CKRD2DIF	Edit the data set names of `UNLOAD` data set to be used.
C2RXDEFU	As supplied with IBM Security zSecure, this member is empty. It is automatically embedded by `CKRXDEF1`. For batch processes that use the `C2RC` resource, this script behaves like the Setup (default) preamble option in the ISPF interface. Within the ISPF interface, the `CKRXDEF1` script and `C2RXDEFU` script are also automatically embedded in the product after the preamble. To perform local additions to the `CKRXDEF1` or `C2RXDEFU` scripts, do the following: • Create a copy`C2RXDEFU` in a data set that is identified by the configuration parameter `WPREFIX` or `UPREFIX`. See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. • To use this script in batch mode, override the procedure `C2RC` or change a local copy to concatenate `&WPREFIX..SCKRCARL` or `&UPREFIX..SCKRCARL` before `&CPREFIX..SCKRCARL`. In the ISPF interface the `WPREFIX` and `UPREFIX` data sets are concatenated automatically, if they exist.

Standard CARLa scripts

The following CARLa scripts are not intended to be customized. They are listed in the order in which they occur in the member list of the library, subdivided into ranges.

CKA* - zSecure Audit for ACF2
These members are part of zSecure Audit for RACF or common to zSecure Audit for ACF2 and zSecure Audit for RACF.

CKADF* - SMF displays
These members are SMF queries. See Chapter 7, “SMF and HTTP Reporting (Events menu),” on page 545.

CKADR* - RACF resource audit displays
These members are displays of AU.S - RACF resource. See Chapter 3, “RACF Audit Guide,” on page 255.

CKADU* - RACF user audit displays
CKADUTRU shows trusted users–users with sensitive access to the Trusted Computing Base. See “TRUSTUSR - Trusted users report” on page 292.

CKADVOLD - DASD volume protection display
CKADVOLD reports on DASD volume protection and sharing. See “DASDVOL - DASD volume report” on page 509.

CKAL$* - Concatenation members
These members include a number of other reports. See Chapter 5, “System Audit Guide,” on page 425 and Chapter 3, “RACF Audit Guide,” on page 255.

CKAL@* - Audit concerns for batch reports
These members are used to generate the **AU.S** audit concern OVERVIEW. They are not designed to be run separately, except CKAL@ALL, which generates the fullOVERVIEW

CKALR* - RACF resource audit batch reports
These members are print format reports of **AU.S - RACF resource**. See Chapter 3, "RACF Audit Guide," on page 255.

CKALU* - RACF user audit batch reports
`CKALUTRU` shows trusted users, that is, users with sensitive access to the Trusted Computing Base. `CKALUTR0` is the concise version of the same report. See "TRUSTUSR - Trusted users report" on page 292.

CKAS* - Field definitions for SMF and other log files
These members contain CARLa DEFINE and DEFTYPE statements to define the layout of fields or logs not supported internally. See "Field definitions for SMF and other log files" on page 590.

CKG* - CKGRACF scripts
These members are for use with CKGRACF, the authorized component of IBM Security zSecure Admin.

CKGX* - CKGRACF scripts
The following CARLa queries that generate CKGRACF command streams are available. These queries can be run with job C2RJXRFR, see "IBM Security zSecure jobs" on page 699:

Sample	Meaning
CKGXLIST	List profiles that require a `CKGRACF` refresh
CKGXREFR	Generate `CKGRACF REFRESH` commands for all profiles that require them
CKGXUSRW	Generate `CKGRACF WIPE` commands for `CKGRACF` data and user data for all applicable user profiles.

The other `CKGXR*` CARLa scripts support the `RECREATE` function. For information, see"R - Recreate a profile" on page 70.

CKRD* - zSecure Admin and Audit (or common) displays
`CKRDSY80` shows system settings and software levels. This script is documented in Chapter 5, "System Audit Guide," on page 425. The other CARLa scripts are documented in Chapter 3, "RACF Audit Guide," on page 255 and Chapter 2, "RACF Administration Guide," on page 51.

CKRL* - zSecure Admin and Audit (or common) batch scripts
`CKRL` is an empty member to prevent JCL errors for `CKRL`*variable* specifications, when the variable is empty.

CKRLSYSM (SMF system-wide settings), CKRLSY13, and CKRLSY80 (System settings and software levels) are documented in Chapter 5, "System Audit Guide," on page 425. The other CARLa scripts are documented in Chapter 3, "RACF Audit Guide," on page 255. CKRLGRPI, CKRLMTX1, CKRLMTX2, and CKRLSCPS are two-pass queries. To start two-pass queries use procedure C2RC2. The others documented there are one-pass queries. To start one-pass queries use procedure C2RC.

CKRR* - Report layouts
These members contain the original layouts for a number of `REPORT` command parameters to provide compatibility with previous versions of the product. If

you do not specify a different layout on a NEWLIST statement, these layouts are automatically embedded as the default layouts for a REPORT command.

CKRV* - Verify scripts

The following CARLa queries for resource analysis or one-time command generation are available.

Member	Meaning
CKRV	Empty member that prevents JCL errors for CKRV *variable* specifications, when the variable is empty.
CKRVDSN	Verifies the consistency and completeness of data set resource protection.
CKRVPROG	Verifies the consistency and referential integrity of program protection.
CKRVPWHC	Generates CKGRACF commands to convert hashed passwords to DES-encrypted passwords
CKRVRACF	Verifies RACF database consistency
CKRVTCB	List and check protection of Trusted Computing Base
CKRVUNIX	Generate RACF commands to populate the UNIXMAP class
CKRVWORM	Reports on globally writable resources, which are potential worm-holes.

CKRX* - Members used by the ISPF interface

The following SAS postprocessing sample is available for use with C2RJXSAS.

Member	Meaning
CKRXCFRQ	Lists connect counts to postprocess with SAS software.

The other CKRXC* members are part of COPY functionality. These are documented in "C - Copy" on page 55.

Member	Meaning
CKRXDEF1	A set of CARLa statements, which includes mostly DEFINE statements. Many CARLa scripts supplied with IBM Security zSecure, as well as the ISPF interface use this script. For example, the JCL procedure C2RC embeds the library in the procedure.

CKRXMCFS provides compatibility with earlier zSecure versions for the MENU command.

The CKRXR* members are part of RECREATE function. See "R - Recreate a profile" on page 70.

The CKRXW* members are configurations for zSecure Visual, the Windows interface for IBM Security zSecure Admin.

C2E* - Tivoli Compliance Insight Manager Enabler for z/OS

These members are used by the Tivoli Compliance Insight Manager Enabler for z/OS for the Tivoli Compliance Insight Manager. For details, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

C2RD* - zSecure Admin and Audit or common displays

C2RDFLD is for the FIELDS command. C2RDRAS and C2RDRASD are used to show RACF global settings (RA.S).

C2RL* - zSecure Admin and Audit common batch scripts
These scripts are used for UNLOAD.

C2RXDEF1
A set of CARLa statements, which contains mostly DEFINE statements. You can use these statements in many CARLa scripts supplied with IBM Security zSecure. The ISPF interface also uses these statements. For example, JCL procedure C2RC embeds it.

Other members in the SCKRCARL data set

The following members of the SCKRCARL library do not contain CARLa scripts:

CKA$INDX - Table of contents
Contains a list of all members in the CARLa library with a brief explanation.

CKA#ZA13
Release notes for zSecure Audit for RACF version 1.13

CKF#MSGS
zSecure Collect messages

CKG#MSGS
CKGRACF messages

CKR#MSGS
zSecure Admin and Audit messages

CKR#ZM13
Release notes for IBM Security zSecure Admin version 1.13

CKR#ZS13
Release notes for zSecure Admin and Audit version 1.13

CKR#Zz13
Release notes for zSecure Admin and Audit version 1.13

CKRL, CKRV
Empty members (to prevent JCL errors)

CKRXCFRS
Postprocess connects with SAS (see job C2RJXSAS)

CKX#MSGS
Messages for the CKX component of zSecure Admin and Audit

C2A#AA13
Release notes for zSecure Audit for ACF2

C2AI*
Control statements and messages for job C2AZJIVP. This job is used for Installation Verification.

C2P*
zSecure Alert messages and mappings

C2R#MSGS
zSecure Admin and Audit messages.

C2RX*
Miscellaneous use.

C2RXCSRT
SORT control statements used by Change Tracking.

C2RXLOG
Input for SCKRPROC C2RSLOG to copy server logs.

C2RXMHD*
Input for SCKRPROC CKACTM (email support).

C2RXSL01
XSLT stylesheet to transform tabular reports to HTML.

CKV#MSGS
Documentation of CKV messages.

Chapter 12. CARLa Command Language

The CARLa Auditing and Reporting Language (CARLa) is a programming language for creating RACF administration and audit reports using zSecure.

Choose from the following options to create, enter, and process CARLa commands:

Batch processing
For batch processing, you can specify CARLa commands in the `SYSIN` input file. You can also pass commands as parameters with the PARM keyword on the EXEC JCL statement. When called under TSO as a command processor, commands can be entered as TSO command parameters. For more information about using CARLa for batch processing, see Chapter 11, "Calling zSecure," on page 689.

Command-line processing
When zSecure is called as a command processor on VM/CMS, you can enter CARLa commands as VM command parameters. For more information about using CARLa for command-line processing, see Chapter 11, "Calling zSecure," on page 689.

ISPF interface

Under ISPF, the CARLa commands are typically generated by the panels. However there are several locations where you can specify your own custom CARLa:

- As an ISPF primary command CARLa.
- From the *xx*.C menu options such as EV.C, you can generate custom reports by specifying limited CARLa that is enhanced with some predefined layouts.
- The CO main menu option provides several possibilities for custom reporting. You can create and maintain your own custom reports and also create and submit single queries to create a one-time report.

`IMBED` and `INCLUDE` statements

Use the `IMBED` or `INCLUDE` command to read additional CARLa commands from files, data sets, or library members. CARLa cannot be used as input to the CKGRACF, the APF-authorized group-administration component. For more information, see Chapter 14, "CKGRACF Command Language," on page 1499.

For more information, see the following topics:

- "CARLa syntax"
- "CARLa command overview" on page 715
- "CARLa command reference" on page 717

CARLa syntax

This topic explains the syntax notation and rules for CARLa commands. It describes:

- The rules to follow when coding commands.
- How to read the notation for the command syntax

For more information, see the following topics:

- "Syntax rules"
- "CARLa syntax diagrams"

Syntax rules

Follow these rules when you code CARLa commands:

- Most commands are made up of a command keyword followed by parameters.
- Separate parameters by using blanks or commas.
- Use the equal sign (=) to assign a parameter a specific value.

  ```
  limit in=10000, out=10
  ```

- You can also specify a value by including the value in parentheses as follows:

  ```
  copy user(model) touser(newuser)
  ```

- For parameters that support it, specify a list of values using parentheses.

  ```
  report redundant, by=(reason, key)
  ```

- For statements that continue to the next line, follow the last parameter on the line with a comma.
- Commands intended for use in the program parameter string do not require parameters, `MARGINS` and `CAPS` for example.
- Use a semicolon at the end of the line to end the command, or use a new line character after the last parameter.

  ```
  select class=program; list memlst
  ```

- The command processor ignores blank spaces that are immediately followed by commas. It also ignores blank spaces on both sides of command keywords.
- Commands like `SELECT` and `SIMULATE` use the same format as the RACF and ACF2 command parameters where a value for a keyword is enclosed in parentheses:

  ```
  simulate setropts protectall(fail)
  select owner(sys1)
  ```

- Enter commands in any case.
- *Empty lines* can be part of a command, as implied by the previous definitions.
- You can specify commands in any order, except when using the `NEWLIST` command.

  This command divides the input into separate list descriptions. In each list description after a `NEWLIST` command, you must specify the selection and print commands (`SELECT`, `EXCLUDE`, and `PRINT`) before specifying any LIST or SORTLIST commands.
- For comment lines, use the `/*` symbols at the beginning of the line. Use the `*/` symbols to end the comment. If the comment crosses a line boundary, the command listing includes an * (asterisk) character behind the line number.

CARLa syntax diagrams

Table 284 describes the notations for the command syntax diagrams in the CARLa command documentation.

Table 284. Syntax notation for CARLa commands

Convention	Meaning
caps	Name of a command, keyword, or variable
italics	Value of a variable
Underlined	Default value

Table 284. Syntax notation for CARLa commands (continued)

Convention	Meaning
[]	Optional item.
{}	Pick one of the enclosed terms.
|	Pick only one of the separated terms.
...	Preceding value can be repeated.

CARLa command overview

Each time you run a command, you must specify at least one of the following main CARLa commands for processing the command output.

UNLOAD
Create a variable blocked copy of all selected records for later processing.

LIST
List the key (name) and optional fields or strings for all selected resources.

SORTLIST
Provides the same information as the LIST command, but the data is sorted in ascending order of the fields listed, with column headers.

DISPLAY
Like SORTLIST, but the data from the command is shown online in an ISPF table rather than being sent to a file. If you use batch mode or if the NEWLIST DISPLAYTOFILE parameter is set, it acts like the SORTLIST command.

(D)SUMMARY
Creates a report or ISPF table summarizing the values and counts of selected input occurrences.

VERIFY
Performs consistency checks on the command input and creates the RACF commands to fix any problems identified in the CKRCMD file.

REPORT
Report information that satisfies criteria not covered by the SELECT command.

(RE)MOVE
Creates RACF commands in the CKRCMD file to remove (or move) users, permits, or whatever is requested by the parameters.

COPY
To generate RACF commands on the CKRCMD file to clone users with their permits.

Use the following commands to select the information for auditing and reporting.

SELECT
To indicate conditions that the occurrence must satisfy to be selected. Multiple parameters on a single SELECT imply an AND function between the parameters - that is, all criteria must be satisfied to cause selection. Use of multiple SELECT statements implies an OR function - that is, any successful SELECT statement causes selection.

EXCLUDE
To indicate conditions that must be satisfied to reject the occurrence. Multiple parameters on a single EXCLUDE imply an AND function between the

parameters - that is, all criteria must be satisfied to cause rejection. Use of multiple EXCLUDE statements implies an OR function - that is, any of the EXCLUDEs matching is sufficient to reject the occurrence.

The following commands also influence the information processed.

ALLOC
To select a set of security databases and CKFREEZE, SMF, or command output files. If omitted, the default is the currently active security database and a small CKFREEZE subset of live control blocks called 'current settings'.

DEFTYPE
Create a custom NEWLIST type for reporting on any type of file.

LIMIT
Limit input, output, or processing to a maximum value. The value can be a number, a discrete or generic value for example.

SIMULATE
Answer what-if questions or provide information missing from the zSecure Collect file.

SUPPRESS
Suppress error messages for certain volumes, catalogs, users, or groups. You can also suppress command creation.

The following commands influence `SYSIN` and `SYSPRINT` characteristics.

CAPS
Force all output to uppercase.

Limitation:

DBCS characters in the output from a `NEWLIST` statement are not affected by the `CAPS` option if the corresponding NEWLIST statement also has a DBCS option specified. In all other cases, including a listing of the input commands, DBCS characters are not preserved.

MARGINS
Specifies which columns to read from `SYSIN`.

MERGELIST/ENDMERGE
Create a report containing several subreports, each with their own selection and format characteristics.

NEWLIST
Create more than one report or output file in one pass.

PRINT
Change print output file options like titles and page length.

A few examples:

```
select class=group, notermuacc
list class key
```

The following commands list all RACF groups with the NOTERMUACC attribute.

```
select operations or special
list class key
```

The following commands list all profiles with the OPERATIONS or SPECIAL attribute. Since no class is specified, both USER and CONNECT profiles are listed.

```
verify dataset protectall indicated
suppress volser=bckup1
suppress volser=bckup2
```

The following commands perform a cross-check of data sets with data set profiles, but excludes two volumes from its analysis.

The remainder of this section describes the syntax and parameters of all commands.

CARLa command reference

The CARLa command reference provides detailed information about each command including command and parameter descriptions, default settings, and any restrictions on a command.

Table 285. List of CARLA commands

ALLOCATE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the ALLOCATE command to select files or dynamically allocate existing data sets for input or output. You can abbreviate the command to ALLOC.

The ALLOC command provides an extensive set of parameters for selecting and allocating files or data sets. The parameters available depend on the command format and the allocation mode. The ALLOC command also provides global parameters that are available for use with any command format or allocation mode.

Syntactically, the ALLOC command has two formats, the *file* format and the *option* format. Specifying any file format ALLOC command activates explicit allocation mode. If you do not specify a file format command, the program activates implicit allocation mode, which is also the compatible with earlier versions.

File format

The file format explicitly defines one input or output file, data set, or live input source per command. The following example shows the syntax for an ALLOC file format command:

```
ALLOC TYPE=type
[DD=ddname] |
[DD=ddname {
  [DSN=dsn|dsn(mem) |
  CMSFILE='fn ft fm'} |
{ DSN=dsn|dsn(mem) |
  DSNPREF=prefix |
  CMSFILE='fn ft fm' |
  SMF |
  ACTIVE |
  [PRIMARY|BACKUP] [ACTIVE|INACTIVE] |
  [PATH='pathname'] |
  FILEDESC=n [PIPE=Y|YES]
  GETPROC=procedure   }
 [VOL=volser UNIT=unit]
 [SUBSYS=(name[.exit[.parm1[.parm2]]])
 [FUNCTION=MERGE|MAIN|BASE]
 [MOD]
 [FILEDATA=RECORD]
 [SVC99]
 [DELETE]
 [COMPLEX=complex]
 [VERSION=version-identifier]
 [NJENODE=nodename]
 [RRSFNODE=nodename]
 [ZSECSYS=system-name][ZSECNODE=node-name]
ALLOC TYPE=type
[DD=ddname {
 CMSFILE='fn ft fm' |
[PRIMARY] }
{
  CMSFILE='fn ft fm' |
  SMF |
 [PRIMARY]
```

```
    [FUNCTION=MERGE|MAIN|BASE]
   [COMPLEX=complex]
   [NJENODE=nodename]
[RRSFNODE=nodename]
```

Note: If the SMF keyword is used, the TYPE keyword can be omitted.

Option format

The *option* format has two kinds of parameters: the *ddname redirection* parameters and the *Live Input Source selectors* for live SMF files and live security databases. The *ddname redirection parameters* include parameters for files that require implicit allocation mode and parameters for files that are not dependent on the allocation mode.

The following example shows the live input source selectors (`SMF`, `LIVE`, `BACKUP`, `ACTIVE`, and `INACTIVE`).

```
ALLOC
[SMF]
[[BACKUP] [ACTIVE|INACTIVE]
  | DB=list
]
```

Global parameters valid with any format or allocation mode

This code sample shows the syntax for the global allocation parameters for any allocation command:

```
ALLOC [INDD=file] [OUTDD=file] [ERRDD=file]
[NOCLOSE]
[CLEANUP] [LETRAPOFF] [LETRAPON] [NOLE]
[NODCBE] [NOCLEANUP] [NODUMP] [NOESTAE]
[STORAGEGC] [TEXTPIPE=n] [NOBSAMBPAM]
[DDSAMPIN=file]
[DDUNLOUT=file] [DDCKR2PASS=file] [DDCKRTSPRT=file]
[CKRCMD_EXEC=EX|REQ|TSO]
```

For parameter descriptions, see "Implicit allocation mode parameters" on page 731 and"Global allocation parameters" on page 729.

The program uses the following default `ALLOC` parameters if no `CKRACF`*nn* files are allocated:

```
ALLOC PRIMARY ACTIVE
```

Usage notes

- If you specify any *file* format `ALLOC` command, *explicit allocation mode* is activated. If you do not specify a file format `ALLOC` command, *implicit allocation mode* is activated.
- Using the ALLOC parameters, the *file* format explicitly defines one input or output file, data set, or live input source per command.
- `ALLOC` commands are processed first, before any data is read and before the `NEWLIST` commands are processed.
- Not all allocation parameters apply to every product.
  - `SMF` and `DDPFXSMF` are for zSecure Audit.
- You can use the following parameters only in implicit allocation mode: `DDUNLIN`, `DDCKRCMD`, `DDPFXSMF`, and `DDPFXDB`. The following example, shows the syntax for these parameters.

```
ALLOC [DDUNLIN=file] [DDCKRCMD=file]
[DDPFXSMF=prefix] [DDPFXDB=prefix]
```

For more information about allocation modes and parameters, see the following topics.

- For file and data set allocation, see "Explicit allocation mode."
- "Global allocation parameters" on page 729
- "Live input source parameters" on page 727
- "Implicit allocation mode parameters" on page 731

Explicit allocation mode

Explicit allocation mode is the *file* format of the ALLOC command. Use the file format to specify one file or data set per ALLOC command and activate explicit allocation mode. Explicit allocation mode means that no files are implicitly allocated that can be allocated explicitly.

COMPLEX= *complex*

Specifies the security complex name. A complex is defined as a number of systems sharing the same physical security database. For example, a complex name can be used to distinguish OLD from NEW or PROD from TEST. The *complex* value can be a maximum of eight characters long.

The default complex name is based on information in CKFREEZE and UNLOAD data sets. Beginning with zSecure V1.12, the default value for COMPLEX is taken from the RRSFNODE name of the system. If the system is not running RRSF or if this information is not available, the default value is taken from the SYSPLEX name. If the SYSPLEX name has the value *LOCAL* or if this information is not available, the default value is taken from the SYSNAME.

Note: Whether the RRSF node name can be obtained, depends on whether a zSecure Server is active or not.

For UNLOAD data sets created using zSecure V1.11 and earlier, the data set contains the security data set names and an SMF SYSID. The security data set name is searched for in the CKFREEZE data with the same VERSION. If the name is found, the complex name is copied. If the name is not found, the system uses either a matching SMF SYSID name or the default system name. See the command DEFAULT.

Note: If a CKFREEZE file is not specified, a default in-storage source is assumed.

The logic used to assign the default complex name is documented in the SYSPRINT by messages in the CKR23*xx* range.

For output files, the names are assigned to complexes based on FUNCTION, and for the rest on a first-come first-served basis. See "FUNCTION" on page 722.

For input data set containing SMF records or Access Monitor records, the sequence of processing is different from that for other input sources. The SYSID is always first searched in the CKFREEZE sources, and each individual record is assigned to the matching COMPLEX. If the SYSID cannot be matched, a specified COMPLEX name is used. If no COMPLEX name has been specified, the SYSID is used as default for the COMPLEX.

DD= *file*
ddname=*file*

This keyword specifies the MVS ddname or CMS file definition for this allocation. Do not specify any reserved ddnames.

DELETE

Deletes the specified data set when processing ends. Processing ends when the

output processing for the TYPE has finished without an abend, attention key, or a return code of 12 or greater. The data set is only deleted if there is a NEWLIST TYPE= command for the specified type, or if there is another reason to read the data. The DELETE specification is implemented for MVS, but does nothing under CMS. The DELETE keyword is mutually exclusive with GETPROC. When the disposition for any file changes to DELETE, the program issues message CKR1357.

DSN= *dataset*
DA=*dataset*
DATASET=*dataset*
Specifies the data set name for dynamic allocation. Enclose the data set name in quotations. You can also include a member name in parentheses. If you omit the quotations, no user ID is prefixed to the data set name specified.

DSNPREF= *prefix*
Use this parameter to require a catalog search for selecting non-VSAM, VSAM cluster, and alias data set names starting with the indicated high-level qualifiers.

Syntax rules

- Do not specify quotations.
- The last qualifier specified is interpreted as a partial qualifier.
- You must specify at least TYPE= with DSNPREF=.
- DSNPREF= is mutually exclusive with the DD, UNIT, and VOLSER parameters.
- To match only full qualifiers, end the DSNPREF value with a period.
- When you specify TYPE=SMF for data sets for the same system, specify the data set names in alphabetic order and that the order matches the chronological order of the SMF records in the data sets. For the Tivoli Compliance Insight Manager Enabler for z/OS users, gaps in the SMF collection can occur if the order does not match.

Processing considerations

- Data sets are added as if ALLOC DSN= was specified with the same properties specified on the ALLOC DSNPREF= statement, unless the data set names are present on an explicit ALLOC DSN= with the same TYPE, FUNCTION, and COMPLEX, or previously added by such an ALLOC DSNPREF=.
- Any data sets found in the catalog are listed in a severity 0 message CKR1353.
- The absence of any matching data set names is not flagged. When both an alias name and the real data set name match with the prefix, the data set is processed twice.
- If no data sets are found, the program does not issue an error message. It continues to process other requests, if they exist. In this manner through repeated invocations of CKRCARLA, an unknown number of files can be processed for each interval, without sudden failures if the number happens to be 0 after some interval. If you specify the DSNPREF parameter, you cannot specify values for the UNIT and VOLUME fields.
- A maximum of 100 data sets can be automatically allocated per NEWLIST type per run. This restriction is due to the way the automatically allocated DDnames are constructed. When the DSNPREF specification finds more than 100 matches, the behavior depends on the NEWLIST type. For TYPE=SMF, a severity 8 message CKR1404 is given; the first 100 SMF files are processed, and any live SMF specification is ignored with a

CKR1405 message. For other NEWLIST types, a severity 12 message CKR1289 is given for any data set beyond 100 per type and the run is terminated. The behavior for TYPE=SMF makes it possible to use the DELETE operand on the ALLOC to remove processed SMF (staging) data sets and pick up the next 100 data sets in a subsequent run.

FILEDESC= *n*
Use this parameter to write an OUTPUT or CKRCMD file to a UNIX file descriptor, *n*. The file descriptor can be part of a pipe. The FILEDESC keyword is mutually exclusive with PATH, UNIT, VOL, and MEMBER.

FUNCTION= *function*
F=*function*

This keyword specifies how the allocated file is to be used. The main usage is when merging or comparing RACF databases or CKFREEZE files.

You can specify the following values for the FUNCTION keyword.

MAIN
For TYPE=RACF or TYPE=UNLOAD files, this value indicates that the database is to participate normally in NEWLIST TYPE=RACF and VERIFY/REPORT commands. This value is the default.

If two or more ALLOC statements specify the same COMPLEX but one has FUNCTION=BASE the other cannot have FUNCTION=MAIN.

MERGE
For TYPE=CKRCMD files, this value indicates that the file is to contain the commands to remove the profiles that have been merged into the current file. F=MERGE is only useful in IBM Security zSecure Admin.

BASE

Indicates that the specified input file is to be used as a baseline in a compare process. The FUNCTION=BASE specification is useful within the context of the following ALLOC types: RACF, UNLOAD, and CKFREEZE.

The use of FUNCTION=BASE is supported with the following Security zSecure entitlements: Admin, Audit, and Alert.

Creating the default COMPAREOPT specification:

To create a default comparison specification that is used when no other COMPAREOPT specification has been defined, use the following ALLOC command: ALLOC FUNCTION=BASE without including a complex name. When this statement runs, it establishes the system-defined COMPAREOPT specification named DEFAULT as the default comparison specification. The default COMPAREOPT is used in the NEWLIST and OPTION statements when no other COMPAREOPT specification is specified. For information about processing and restrictions, see "COMPAREOPT processing rules ."

For more detailed information about the Default COMPAREOPT specification, see "Compare processing" on page 46.

Processing rules
The following processing rules and restrictions apply to the ALLOC FUNCTION=BASE option.

ALLOC statement rules

- If two or more ALLOC statements specify FUNCTION=BASE, but use a different complex name, an error message is issued. After parsing the input commands, the processing is stopped.

- If two or more ALLOC statements specify the same COMPLEX and one includes the FUNCTION=BASE parameter, the other statement cannot include the FUNCTION=MAIN option.
- If a TYPE=CKFREEZE NEWLIST is specified with the FUNCTION=BASE option, then the ALLOC statement for the security database of the matching complex must also specify that option. If the option is not specified in both ALLOC statements, an error message is issued.

Establishing default settings for the COMPAREOPT statement

- The statement ALLOC COMPLEX FUNCTION=BASE establishes the default COMPAREOPT specification for the BASE keyword for the COMPAREOPT statement. That is, COMPAREOPT BASE=DEFAULT.
- The statement ALLOC FUNCTION=BASE establishes the default COMPAREOPT specification for *all* NEWLISTs and OPTION statements. That is, if any NEWLIST or OPTION statement requests a compare operation without specifying a COMPAREOPT, the system uses the DEFAULT COMPAREOPT.

  If a NEWLIST or OPTION statement specifies a compare operation without including a COMPAREOPT specification, and the DEFAULT compare specification has not been established, an error message is issued.
- The DEFAULT COMPAREOPT specification is not supported on the following NEWLIST types:
  - ACCESS
  - DASDVOL
  - FIELD
  - FIELD_OVERRIDE
  - MERGE
  - NEWLIST
  - REPORT types: REPORT, REPORT_AC1, REPORT_NONDEFAULT,REPORT_OUTOFGROUP, REPORT_PADS,REPORT_PROFILE, REPORT_REDUNDANCY, REPORT_SCOPE, REPORT_SENSITIVE
  - SMF
  - TEMPLATE
  - TYPE

  You can still perform compare operations on these NEWLIST types, but you must explicitly specify the COMPAREOPT statement.

  If you specify ALLOC FUNCTION=BASE, the display or report output contains information from all relevant input sources. However, for the NEWLIST types that do not support compare processing, the COMPARE_CHANGES or COMPARE_RESULT fields are reported as missing. Although these NEWLISTs do not support the default COMPAREOPT specification, you can use an explicit COMPAREOPT statement to do a comparison.

FILEDATA=RECORD

Opens the UNIX file, specified by PATH='*pathname*', as a record file. A record file is a binary UNIX file consisting of a number of records, each preceded by a 4-byte word specifying the length of the record. Using the FILEDATA=RECORD parameter, DEFTYPE files can be opened for input of records and TYPE=OUTPUT files can be opened for output of records.

When zSecure opens a UNIX file to read or write a RACF database unload, SMF unload, or CKFREEZE structure, the FILEDATA=RECORD parameter is not required. zSecure assumes that UNLOAD and CKFREEZE files are always in the record format.

z/OS V1.12 and later supports UNIX record type files. For UNIX record type files on these z/OS versions, the FILEDATA=RECORD parameter on the ALLOC command is not required because zSecure opens them as record files even if the ALLOC FILEDATA=RECORD parameter is not specified. For TYPE=OUTPUT files on z/OS V1.12 and later, you must always specify the FILEDATA=RECORD parameter on the ALLOC command in order for zSecure to open them as record files.

For z/OS 1.12 and later, it is possible to specify FILEDATA=RECORD files by using DD statements in JCL. When FILEDATA=RECORD files are specified in JCL, CARLa does not support reading or writing records that exceed 32760 bytes. To support FILEDATA=RECORD records that exceed 32760 bytes, specify FILEDATA=RECORD files by using ALLOC statements in CARLa instead of DD statements in JCL.

z/OS V1.11 and earlier versions do not support UNIX record type files. For UNIX files on these earlier versions, always specify FILEDATA=RECORD files by using ALLOC statements in CARLa instead of DD statements in JCL. For z/OS V1.11 and earlier, to open a DEFTYPE or TYPE=OUTPUT file in FILEDATA=RECORD format always specify the FILEDATA=RECORD parameter on the CARLa ALLOC statement.

GETPROC= *procedure*
Specifies the name of an external module for supplying the data for this type. The maximum length of the module name is eight characters. This keyword is intended for internal use only.

MOD
Appends output to an existing data set or z/OS UNIX file. The `MOD` keyword is only valid for non-partitioned data sets of `TYPE=CKRCMD` and `TYPE=OUTPUT`. It is only effective when used in combination with the `DSN=` or `PATH=` parameter.

NJENODE= *complex*
Specifies the name for the NJE node where jobs with commands should be sent. The name can be up to eight characters long. If you use `CKFREEZE` files, you do not need to specify the `NJENODE` because the `CKFREEZE` files contain the node information. However, the node information might be missing if there is a JES release support problem.

PATH= *pathname*
Specifies the z/OS UNIX path name. This keyword is an alternative for `DSN=` and `CMSFILE=`. The maximum path name length supported is 1023. When you specify this parameter with the `SVC 99` parameter, only the first 255 bytes of the path name are used; relative path names are not supported.

PIPE=YES
Use this keyword with `FILEDESC=`*n* to indicate that the output file descriptor must be explicitly closed. If this keyword is not specified for pipes, the other side of the pipe continues waiting on the pipe.

RRSFNODE=*node-name*
The name of the RACF remote sharing node where commands can be sent. The maximum length of the `node-name` is eight characters. You can leave this parameter blank if `CKFREEZE` files are used. This parameter is not currently in use.

VERSION

This keyword is used to classify the data allocated into separate sets such as OLD and NEW. The maximum length of the version identifier is four characters. This value is different from the COMPLEX value. The COMPLEX value is used to identify the systems that have a shared RACF database and that are the source of the data. You can use the VERSION specification to analyze data in the same COMPLEX at multiple points in time.

The VERSION keyword influences how CKFREEZE and security sources are grouped together into complexes. Generally, different VERSIONs are handled as separate complexes. A separate VERSION causes the old and new versions of a physical DASD volume to be interpreted as different volumes based on the point in time when the data is analyzed. A separate VERSION also causes RRSF sysplexes to be treated as different sysplexes even though the RRSF node names are the same. However, if you want to perform point-in-time analysis, use a different name for the COMPLEX even if you specify a VERSION. Many reports only show 8 characters of the complex name which does not include the VERSION identifier. If you use the same COMPLEX name, you cannot use the report to identify the data from different versions. If you write your own CARLa program for generating the report, the VERSION is shown in the report output if you specify an output length modifier of 13 or greater on the COMPLEX field. See "Modifying output length" on page 797.

ZSECNODE=*node-name*

Specifies the node name for locating the specified data set. The maximum length of the *node-name* is eight characters. This value corresponds to the node name specified in the network configuration file. The *node-name* specification applies to a RACF database that is shared between multiple systems. When using the ZSECNODE parameter, zSecure uses the preferred server that is designated in the zSecure configuration file to access the specified data set. The special value asterisk (*) specifies that all defined ZSECNODEs are used. The special value period (.) specifies that the current ZSECNODE is used.

If both ZSECSYS and ZSECNODE are specified, zSecure verifies that the specified system is defined as a member of the specified node. If the specified system is not a member of the specified node, zSecure issues an error message and the program stops.

Note: Sensitive fields that are present in UNLOAD data are not sent across the zSecure network.

ZSECSYS=*system-name*

Specifies the system name for locating the specified data set. The maximum length of the system-name is eight characters. This value corresponds to the system name specified in the network configuration file. The system name specification applies mainly to system-specific data sets like a CKFREEZE or an SMF data set, but it can also be used for a RACF database. zSecure locates the specified data set using the server on the specified system.

The special value asterisk (*) specifies that all defined ZSECSYS systems are used. The special value period (.) specifies that the current ZSECSYS is used. If both ZSECSYS and ZSECNODE are specified, zSecure verifies that the specified system is defined as member of the specified node. If the specified system is not a member of the specified node, zSecure issues an error message and the program stops.

SUBSYS=(*name***[,***exit***[,***parm1***[,***parm2*

Directs the allocation to the subsystem specified in the first positional

subparameter. The *name* has a maximum of four characters. The syntax for the rest of the subparameters depends on the subsystem.

Usage notes

- The syntax is like that of the SUBSYS parameter on the JCL DD statement. The maximum length of the subparameters supported is 67. You can specify the subparameters enclosed in three types of quotations. Quotations are required when a subparameter uses parentheses, commas, equal signs, or blank characters. By default the subparameters are passed to DYNALLOC as is, without changing the case. To avoid an IKJ5623I error, check that the subparameters are supplied in the correct case.
- For the LOGR subsystem, the second subparameter is an exit name, IFASEXIT for SMF log streams for example. The syntax for the rest of the subparameters can be found in the *z/OS MVS JCL Reference*.
- zSecure recognizes the LOGR subsystem and converts all subparameters to uppercase before supplying them to DYNALLOC.
- The DSN= parameter can be used to pass the log stream name.
- You must have READ access on the stream name specified in SAF class LOGSTRM. Otherwise, the system abends with a 913-74 error.
- SMF NEWLIST supports reading from SMF log streams.

SVC99

Request DYNALLOC (SVC99) and QSAM/BSAM I/O simulation instead of using more efficient UNIX open/close and direct UNIX I/O. You only need this parameter if the ddname is for passing to other components and you want an EBCDIC file.

If you use ENCODING=UTF-8 on an SVC99 allocated UNIX file, you get an unusable file because QSAM I/O emulation writes EBCDIC newline characters (X'15') between the UTF-8 records.

TYPE= *type*

Specifies the file or data set type to allocate. The following types are supported:

Table 286. File types for allocating data sources for zSecure

TYPE	Description
ACCESS	Type for allocating a data set for Access Monitor records from the RACF database cleanup function in zSecure Admin. This file is used by the ACCESS NEWLIST, and RACF_ACCESS NEWLIST. For details, see "ACCESS: Access Monitor Records" on page 953.
ACF2RULE ACF2INFO ACF2LID ACF2	
CKFREEZE	Type for allocating a data set to capture the zSecure Collect data required for RACF administration and auditing using zSecure.
CKRCMD	File type for generated commands created as a result of COPY, MOVE, REMOVE, or VERIFY operations.
DEFTYPE TYPE=*type*	You can use the DEFTYPE command for defining NEWLIST type for custom reports. For more information, see "DEFTYPE" on page 777.

Table 286. File types for allocating data sources for zSecure (continued)

TYPE	Description
INPUT OUTPUT	Use these types for general allocation of files for purposes like providing DD=CKRCARLA input or an output file for z/OS Unix that receives the data from a NEWLIST DD= statement. Use these file types with the DD= parameter to immediately allocate the file. If you do not specify the DD= parameter, the file is allocated later and cannot be used IMBED command processing.
RACF	Use this specification to allocate a RACF database. The database can be the RACF database of the system your job is running under (ACTIVE, PRIMARY, or BACKUP), a copy of the database, or of a foreign database that is in use by another z/OS or z/VM image (or by multiple images). For foreign databases and database copies, combine TYPE=RACF with a specification of the DATASET. In order to allocate a RACF database that consists of multiple data sets, specify multiple TYPE=RACF allocations for a single complex in the same order as the data set names occur in RACF data set name table ICHRDSNT. See "RACFDSN - RACF Data Set Name Table ICHRDSNT" on page 275. Note that allocating a RACF database incurs the risk that the database can be updated while zSecure is reading the database. To avoid this risk, use an UNLOAD data set.
SMF,SMFSTREAM	Use TYPE=SMFSTREAM for allocating an SMF log stream. This file is for SMF NEWLIST processing. You cannot specify parameters to limit the number of returned SMF records. If you must specify a limit, use TYPE=SMF with the SUBSYS keyword.
UNLOAD	Use TYPE=UNLOAD for allocating the file that stores the unloaded RACF data read from the live RACF database. During the unload process, zSecure copies the data to the UNLOAD file in a proprietary format suitable for high-speed searches.

In previous releases, TYPE=IOCONFIG is an alias for TYPE=CKFREEZE. TYPE=CMDOUT is an alias for TYPE=CKRCMD. TYPE=CKRUNL is an alias for TYPE=UNLOAD. Messages and explanations generally use the latter names.

UNIT= *unitname*
U=*unitname*
Unit name to use in combination with the volume serial to indicate the device where the data is stored. You must specify this parameter with the VOLUME.

V= *volume*
VOL=*volume*
VOLSER=*volume*
Volume to use in the dynamic allocation request. You must specify this parameter with the UNIT parameter with the volume serial.

Live input source parameters

ACTIVE
Use this parameter to select active (live) data as the data source for zSecure. ACTIVE is the default setting. You can use this parameter in both implicit allocation mode and explicit allocation mode. For zSecure Admin for RACF and zSecure Audit for ACF2, the following file types are valid: TYPE=RACF, TYPE=CKFREEZE, and TYPE=SMF.

For zSecure Audit for Top Secret, the following file types are valid: TYPE=CKFREEZE and TYPE=SMF.

For TYPE=SMF, the processing depends on whether SMF is recording to data sets or to log streams. If logging is done through data sets, all SMF recording data sets are allocated. If logging is done through log streams, all currently active SMF log streams are allocated. The SMF log stream file allocation sets the parameters DURATION=(24,HOURS), and SID(*name*) where *name* is the SMF ID of the current system.

The program must be able to find the specified log stream names. The log stream names can be located if you call the program in APF mode–through CKRCARLX for example, or if you connect to a recent CKFREEZE file with the specified SMF log stream settings. The CKFREEZE file must be part of the default complex.

Note: The SMF recording data sets or SMF log streams are only allocated if you specify an SMF NEWLIST.

BACKUP
Use this keyword to select the live backup database as input. Using BACKUP instead of ACTIVE can be used to reduce the I/O load on the primary security database.

DB= *n*
DB=(1,*n***,...) DATABASE=...**
Selects the RACF database sequence numbers. You must include sequence Number 1 for the master data set. The DB parameter must return number or a list of numbers. The highest number supported is 64. A maximum of 64 numbers can be combined in one run. The database sequence numbers are defined in the database name table, see the NEWLIST TYPE=DSNT. You can only specify the DB parameter on an ALLOC command in implicit allocation mode.

INACTIVE

Selects an inactive security database from the live system as the data source.

PRIMARY
PRIM
Selects the live data as the data source for zSecure. In implicit allocation mode, PRIMARY is the default data source selection.

SMF

Allocate SMF to allocate the live data source.

If SMF logging is being done to files or data sets, the SMF recording data sets are allocated, typically SYS1.MANx for example.

If logging is done through log streams, all currently active SMF log streams are allocated with the parameters DURATION=(24,HOURS) and SID(*name*). The *name* is the SMF ID of the current system. The program must be able to find the log stream names by either calling the program in APF mode through CKRCARLX for example, or by connecting a recent CKFREEZE file with the SMF log stream settings. The CKFREEZE file must be part of the default complex.

Note: The SMF files are only allocated if you specify a NEWLIST TYPE=SMF statement.

In implicit allocation mode, any SMF file previously allocated to ddnames SMF00–SMF09 is freed if the ddname is reused for a live SMF data set. SMF files

previously allocated to ddnames SMF or SMF10 and up, are not freed. The allocated data sets are used by zSecure Audit for ACF2. You can have gaps in the range SMF00–SMF09, but no gaps in the range SMF10 and up. For example, if you allocate SMF03, SMF05, SMF10, SMF11, and SMF15, the program does not process the SMF15 ddname.

In explicit allocation mode, specifying TYPE=SMF is equivalent to TYPE=SMF ACTIVE. The program does not use any data sets other than the SMF data set explicitly specified on an ALLOC command and the live SMF data source implied by this operand.

You can combine the Live input source parameters to select the data sets for the SMF data source.

Global allocation parameters

CKRCMD_EXEC= *target*
CMDOUT_EXEC= *target*
This parameter sets the target for commands written in CKRCMD. It can be TSO, EX, or REQ. The default is TSO. There is no separate target string for CKX, because this program is compatible with TSO. If EX is selected, RACF and IDCAMS commands are prefixed with CMD EX. If REQ is selected, RACF and IDCAMS commands are prefixed by CMD REQ. However, not all commands are supported by CKGRACF CMD REQ. This parameter is honored for all commands that are written to CKRCMD and accompanied by a message (as the result of a CARLa command). It does not apply to action commands under ISPF that can queue commands to CKRCMD.

CLEANUP
Forces an unconditional abend intercept and storage cleanup even though not running under ISPF. It is mutually exclusive with NOCLEANUP. The abend intercept is activated after the main input parse is complete. This behavior is in contrast to the default abend intercept cleanup behavior for ISPF which is activated before the main input parse. The intercept stops before the runtime system stops.

DDCARLA= *ddname*
DDSAMPIN= *ddname*
The *ddname* to be used as the default file for embedding members. It overrides CKRCARLA.

DDCKR2PASS= *ddname*
DDCNROUT= *ddname*
The *ddname* for queued CARLa command output. That is, CARLa commands that have been queued by line commands. If a ddname is specified by the DDCKR2PASS= parameter, the value overrides the ddname specified in the CKR2PASS parameter that is used otherwise.

DDCKRTSPRT= *ddname*
DDCNXOUT= *ddname*
The *ddname* to receive command output from TSO commands called by Security zSecure. If specified, this parameter overrides the CKXT@PRT ddname used otherwise.

DDUNLOUT= *ddname*
The *ddname* to be used as the target for unloading a security database. If specified, this parameter overrides the CKRUNLOU ddname used by default.

ERRDD= *ddname*
Redirects the SYSTERM to the specified *ddname*. You can use this parameter only on the PARM string. You cannot use it as a command in an input file.

INDD= *ddname*
Redirects the SYSIN file to the specified *ddname*. You can use this parameter only on the PARM string. You cannot use it as a command in an input file.

LETRAPOFF
This parameter is only valid on the PARM string. It can be used to turn off the Language Environment abend trap for diagnostic purposes. If NOLE has also been specified, this parameter is ignored. This parameter takes precedence over LETRAPON. If LETRAPON is also specified, it is ignored. Use this parameter only at the request of IBM software support.

LETRAPON
This parameter is only valid on the PARM string. It turns on the Language Environment abend trap for diagnostic purposes. If you also specify the LETRAPOPFF or NOLE parameters, this parameter is ignored. Use this parameter only at the request of IBM software support.

NOBSAMBPAM
This parameter is only valid on the PARM string. It can be used to disable use of the BSAM and BPAM access methods by the program–the program uses QSAM instead. Use of this parameter is only intended for use at the request of IBM software support.

NOCLEANUP
This parameter is only valid on the PARM string. It passes on debugging purposes to pass on abends to ISPF instead of recovering from them. It is meant to be used at the direction of IBM software support if the attempt to clean up the abend causes additional errors. You can find this option in the ISPF interface under SETUP TRACE as: Pass abends to ISPF.

NOCLOSE
Prevents the closing and freeing of data sets during abend recovery processing. You can specify this parameter in the parameter string (the PARM keyword in JCL). Use of this parameter is only intended for use at the request of IBM software support. You can find this option in the ISPF interface under SETUP TRACE as: Prevent closing/freeing data sets during abend recovery.

NODCBE
Prevents 31 bit mode from being used for file I/O processing. You can specify this value in the parameter string (the PARM keyword in JCL). Do not use this parameter unless IBM software support asks you to do so.

NODUMP
Suppresses a system dump. This parameter is only valid on the PARM string. Do not use this parameter unless IBM software support asks you to do so.

NOESTAE
Use this parameter to suppress error traps during the debugging process. This parameter is only valid on the PARM string. Using this parameter can cause Security zSecure to stop working. You can specify this parameter on the PARM. You can also set the option from the Setup Trace menu in the product by selecting **Suppress error traps**.

NOLE
Use this option to turn off Language Environment processing. This parameter is only valid on the PARM string. If this parameter has been specified, the

parameters LETRAPON and LETRAPOFF are ignored. You cannot send SNMP traps if Language Environment processing is turned off.

OUTDD= *ddname*
This parameter can be specified in the parameter string (the PARM keyword in JCL) to redirect SYSPRINT to the specified *ddname*. The parameter cannot be used with an input file.

STORAGEGC
This parameter is valid on the PARM string only. It can be used to turn on garbage collection during the run. In some cases, this setting reduces storage consumption but increases CPU usage.

TEXTPIPE= *n*
Sends all remote text files through a UNIX pipe. This parameter is only valid on the PARM string.

Implicit allocation mode parameters

DDPFXDB= *prefix*
Specifies the prefix for RACF input ddnames. It overrides the default CKRACF. You can specify a prefix of up to six characters. RACF input is read from *prefixnn*, where *nn* is a value in the range 01 – 64, inclusive. The prefix is only used in implicit allocation mode.

DDPFXSMF= *prefix*
Specifies the prefix for SMF input ddnames. It overrides the default SMF. The prefix value can have up to six characters. SMF input is from files *prefix* and *prefixnn*, where *nn* is a value in the range 00 – 99, inclusive. The prefix is only used in implicit allocation mode.

DDCKRCMD= *ddname*
DDCKRCMDOUT= *ddname*
The DDCKRCMD and DDCKRCMDOUT fields contain the ddname parameters for TSO or RACF command output. The ddname values can be generated by COPY, MOVE, REMOVE, and VERIFY operations. If specified, the DDCKRCMD value overrides the CKRCMD file for all NEWLIST commands that produce output for CKRCMD. A NEWLIST statement with F=CKRCMD also writes that output to the specified ddname. The file is read only in implicit allocation mode and applies only to the first security complex.

DDUNLIN= *ddname*
Specifies the *ddname* of the unloaded database for the zSecure data source. The value overrides the value specified in CKRUNLIN program. The file is only read in implicit allocation mode.

If you are uncertain what the resulting allocation would be, review message CKR0615 from the IN.M function on the product menu. This message shows the way that files are assumed to be connected to complexes.

Example - allocate live SMF

The SMF parameter is used with the SMF NEWLIST to allocate the live MVS data sets (usually SYS1.MANx) to SMF ddnames SMF00 and up. The use of this parameter is shown in the following example:

```
/* Allocate live SMF data sets */
alloc smf
```

Example - allocating and limiting an SMF log stream

The following example illustrates how to read SMF records from Oct 15, 2007 for system MYST from an SMF log stream:

```
alloc type=smf dsn=IFASMF.MAIN,
 subsys=(LOGR,IFASEXIT,'FROM=(2007/288),TO=(2007/288),LOCAL',
 'SID(MYST)')
```

Example - use back-up RACF data sets

To minimize impact on system operation, one might read the backup database instead of the primary. For most purposes except statistics, the information in the backup is identical to the primary. Use the following command to read the backup database.

```
alloc backup
```

Example - allocations for combined reports

To report with NEWLIST TYPE=RACF on SYS2 and SYS1 specify the following commands.

```
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE
ALLOC TYPE=UNLOAD   DSN=my.SYS2.UNLOAD
ALLOC TYPE=CKFREEZE DSN=my.SYS2.CKFREEZE
```

Note: COMPLEX parameters are not needed if matched UNLOAD and CKFREEZE files are used.

Example - allocations with RACF databases

You must use the COMPLEX parameter to create RACF reports (NEWLIST TYPE=RACF) on SYS2 and SYS1 using RACF database copies:

```
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE
ALLOC TYPE=RACF     DSN=my.SYS1.RACFDB   COMPLEX=SYS1
ALLOC TYPE=CKFREEZE DSN=my.SYS2.CKFREEZE
ALLOC TYPE=RACF     DSN=my.SYS2.RACFDB   COMPLEX=SYS2
```

Example - allocations for compare

To create RACF reports (NEWLIST TYPE=RACF) for different snapshots of a system (SYS1), specify the following commands. In this example, the COMPLEX parameter is required because the UNLOAD and CKFREEZE files are all from the same system. Without the COMPLEX parameter, the program only processes two of the four files.

```
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD(-1)     COMPLEX=LASTWEEK
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE(-1)   COMPLEX=LASTWEEK
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD(0)      COMPLEX=THISWEEK
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE(0)    COMPLEX=THISWEEK
```

Note: COMPLEX parameters are now required because the system names are the same for all complexes.

Example - allocations for merge

To merge SYS2 into SYS1 specify the following commands.

```
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE
ALLOC TYPE=CKRCMD   DSN=my.SYS1.CKRCMD
```

```
ALLOC TYPE=UNLOAD   DSN=my.SYS2.UNLOAD FUNCTION=MERGE
ALLOC TYPE=CKFREEZE DSN=my.SYS2.CKFREEZE
ALLOC TYPE=CKRCMD   DSN=my.SYS2.CKRCMD FUNCTION=MERGE
```

Note: COMPLEX parameters are not needed if matched UNLOAD and CKFREEZE files are used.

Example - allocations for internal merge

To merge with rename inside a system SYS1 specify the following commands.

```
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD
ALLOC TYPE=CKFREEZE DSN=my.SYS1.CKFREEZE
ALLOC TYPE=CKRCMD   DSN=my.SYS1.CKRCMD
ALLOC TYPE=UNLOAD   DSN=my.SYS1.UNLOAD  FUNCTION=MERGE
ALLOC TYPE=CKRCMD   DSN=my.SYS1.CKRCMD2 FUNCTION=MERGE
```

Note: COMPLEX parameters are not needed if matched UNLOAD and CKFREEZE files are used.

Example - allocating a <deftype> file

```
DEFTYPE TYPE=EMAIL
ALLOC TYPE=EMAIL DSN=HR.PERSONEL.EMAIL
```

BDAMQSAM

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•		

This command can be used to deactivate EXCP I/O to the RACF database and use BDAM and QSAM access methods instead. Under VM, this is the only supported mode of operation. The main purpose of this command is to debug problems. Specifying this command also deactivates fast access through the index. However, if that is the only reason for using the BDAMQSAM command, it is better to use the SUPPRESS INDEX command.

BUNDLE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command can be used to group the output of multiple NEWLIST commands together such that all output is generated per distinct value of the BUNDLEBY parameter. For example, the BUNDLEBY parameter allows you to bundle relevant information per department. The NEWLIST group is terminated by an ENDBUNDLE command. The BUNDLE...ENDBUNDLE group can include MERGELIST....ENDMERGE groups. The merged result is treated as a single NEWLIST. The output for each bundle begins on a new page unless it is emailed. If the email option is selected, separate emails are sent for each bundle. If the PAGERESET option is specified (on OPTION, BUNDLE, or the first NEWLIST within the BUNDLE) each bundle restarts its page numbering at 1. Within each bundle, the NEWLISTs display in the order specified. The resulting reports contain the actual BUNDLEBY value in the title, behind the NEWLIST source time stamp. NEWLISTs of different types can be combined into one bundle. BUNDLE commands cannot be nested.

The LIST, DISPLAY, and DSUMMARY commands are not permitted within a bundle. Only commands that generate output and permitted are SORTLIST and SUMMARY. SUMMARY requests for a NEWLIST are applied to the set of records for each BUNDLEBY value separately. For example, if you are generating output per department, each department gets its own summaries.

The BUNDLE command is closely related to NEWLIST and OPTION, in the sense that OPTION parameters can also be included on the BUNDLE command. See "OPTION" on page 856. The OPTION parameters specified on the BUNDLE are local to the BUNDLE...ENDBUNDLE group. They are the default for each NEWLIST in the group, while each NEWLIST can specify overriding parameters that apply to that NEWLIST only. The MAILTO= option is not supported for a bundle. Use the BUNDLEMAILTO= instead. Mail options apply to the bundled output, not the individual NEWLISTs; therefore, they cannot be specified on commands between BUNDLE and ENDBUNDLE.

BUNDLEBY= *variablename*
Request the output to be bundled per distinct value of the specified *variablename*. This *variablename* can either be a field name or a name used with the DEFINE...AS command. The BUNDLEBY option can also be specified on the OPTION command (defining a default) or on a NEWLIST command. If it is specified on a NEWLIST command, it applies only to that NEWLIST type.

The *variablename* can evaluate to a different variable per NEWLIST type. The most effective bundling method is to issue global DEFINEs with the same variable name for each NEWLIST type, and then specify that variable name in the BUNDLEBY parameter for the BUNDLE statement.The values of the BUNDLEBY variable are bundled by their internal representation. The bundle sort order is the same as for SORTLIST. A BUNDLEBY specification is ignored outside a BUNDLE.

BUNDLEMAILTO= *expression*
BMT=*expression*
Request the bundled output to be emailed to the group responsible for each part of the report. This parameter can only be specified on the BUNDLE command. The expression must be a set of field manipulation functions, see "Field value manipulation" on page 760 based on the BUNDLEBY variable. The resolved string is interpreted as an address list conforming to RFC (2)822, with some restrictions. The restrictions are documented with option MAILTO, see 860. If the expression does not resolve, the email address specified on the ERRORMAILTO parameter is used. See "ERRORMAILTO" on page 859. The subject of the resulting emails is based on the title or toptitle specified on the first nonempty NEWLIST in the BUNDLE, with the BUNDLEBY value appended.

Note: When using any of the MAILTO commands, be sure to specify correct SMTPWRITER and SMTPCLASS options, or include a C2REMAIL DD-statement with an allocation to the SMTP writer, see "C2REMAIL" on page 702. Additionally, be sure to include at least one sender address on either the FROM, REPLYTO, SMTPMAILFROM, or ERRORMAILTO keyword. Also be aware that the email function of Security zSecure is not intended to be used in combination with the INFOPRINT email support as introduced in z/OS V1R5.

Example - emailing bundled output to departmental managers

In this example, the site stores department contact information in a file with records containing the names of the departments and the email addresses of the

responsible managers, separated by a colon. The following code sample, shows the CARLa statements for distributing zSecure reports using this departmental contact list.

```
DEFTYPE TYPE=email
DEFINE TYPE=email dept AS WORD(RECORD,1,':')
DEFINE TYPE=email address AS WORD(RECORD,2,':')
ALLOC TYPE=email DSN=my.email.address.file
//*Insert appropriate DEFINEs for owner in each
//* NEWLIST type used in the BUNDLE where it is not a field
//* or you want to change the to override the default meanin//* g.
 //* Insert the required BUNDLEBY statement.BUNDLE BUNDLEBY=owner
BUNDLEMAILTO=BUNDLEBY:email.dept.address

<>
//* Insert the NEWLIST blocks that specify the reports for bundling.
ENDBUNDLE
```

This specification bundles the output per value of **owner**, and then for each bundle look for the record in **my.email.address.file** that starts with this value, and then take the email address specified for it after the colon and send the bundle there.

The OWNER field is not required on the SORTLIST/SUMMARY statement. That is, you can use a field or variable for bundling without including it in the reports.

Example - bundling NEWLISTs

This example shows how to bundle reports by department on a site where the RACF database is organized in the following way. Each RACF group that follows the SYSUSER group defines a department. Each department group contains among others a user-owning group that owns all user IDs of the department. In addition, the department group contains authorization groups giving access to the departmental applications. The departmental report covers both RACF data and SMF data (available in zSecure Audit for ACF2 only), and bundles three reports: data on the department (RACF), data on invalid password attempts on user IDs of the department, and connects to the departmental authorization groups.

```
  /* define default bundle selector */
define type=racf department(8) as key,
       where class=group owner=sysuser
define type=smf department(8) as user:owner:owner,
       where user:owner:owner:owner=sysuser


  /* a bundle for each department */

bundle bundleby=department f=ckreport,
       tt='Departmental report'

n type=racf name=XXXstart t="Information on department",
  pagereset, pagealign=4
  s class=group owner=sysuser
  sortlist key(8,"Department") instdata("Data from RACF"),
         / "user:   " userid userid:pgmrname,
         / "subgrp: " subgrpnm subgrpnm:instdata,
         /

n type=smf name=XXXlogpw t="Invalid password attempts"
  s type=80 event=racinit(1) exists(department)
  sortlist user,
           user:pgmrname("Info from RACF"),
           date time,
           '  /*' recorddesc


n type=smf name=XXXautha t="Authorisation add"
  define department(8) as racfcmd_group:owner,
         where racfcmd_group:owner:owner=sysuser
  s type=80 event=connect exists(department)
  sortlist racfcmd_group("AuthGroup",9),
           racfcmd_group:instdata("Info from RACF"),
           user("Administrator",13),
           racfcmd_user("User"),
           racfcmd_user:pgmrname("Info from RACF"),
           date time,
           '  /*' racfcmd(wrap,hor,0)


endbundle
```

CAPS

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the CAPS command without parameters to force all subsequent SYSPRINT output to uppercase. This command is useful if your print chain does not print lowercase characters. The output containing a listing of the input commands up to and including the line containing the CAPS parameter is not converted to uppercase.

To print reports in uppercase, use the OPTION CAPS command, see “PRINT” on page 870.

Limitation: DBCS characters in the output for a NEWLIST statement are not affected by the CAPS option if the corresponding NEWLIST statement also has a DBCS option. In all other cases, including a listing of the input commands, DBCS characters are not preserved.

CONVERSION

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The primary usage of conversion rules or conversions is to consolidate similar data during Access Monitor data set consolidation. The CONVERSION command is used to define conversion rules that can replace name segment qualifiers of SUMMARY key fields with fixed characters, if the Access Monitor record matches a selection criterion. Conversion rules have global scope and they are identified by name and NEWLIST type. Conversion rules can be used only in commands that follow the CONVERSION command in the query.

The CONVERSION command (abbreviated as CONV) has the following basic syntax.

```
CONVERSION
   [ TYPE=type ]
   name
   actions
   [ WHERE clause ]
```

TYPE
The TYPE=*type* parameter is optional. It defines to which NEWLIST type the conversion applies. The default type is the ACCESS NEWLIST. The RACF NEWLIST is not supported.

name
The conversion identifier. The TYPE=*type* and *name* form an identification key for the conversion.

actions
The list of actions to be performed on the summary key value. This list has the following syntax:

```
REPLCHAR((subfield,char)[,(subfield,char),...])
```

The *subfield* identifies a qualifier in a SUMMARY key field and can be one of the following identifiers.

Identifier	Description
QUAL*n*	Refers to qualifier *n* of the summary key; *n* is a number from 1 to 123. If the field value is aaa.bbb.ccc, then QUAL1 is aaa, QUAL2 is bbb, and so on.
LASTQUAL	Refers to the last summary key qualifier. If the field value is aaa.bbb.ccc, the LASTQUAL is ccc.
SUBSTRING	Refers to a part of a subfield: QUAL*n* or LASTQUAL. The SUBSTRING has the following syntax: `SUBSTRING(QUALn | LASTQUAL , startpos, length)` The *startpos* is the start position of the substring of the subfield. You can express the length using a *length* or *endpos* variable. For format details, see "SUBSTRING, SUBSTR" on page 763 in "Field value manipulation" on page 760. The command abbreviation is SUBSTR.

WHERE

The optional WHERE clause is an expression that is formed like a SELECT clause for the NEWLIST type=*type* and uses the same fields, relationship operators, and so on. The WHERE clause is evaluated before the conversion is applied. If the evaluation result is TRUE, the conversion is applied; otherwise, it is skipped. Additional field manipulation functions are defined for this clause in the CONVERSION context, see QUALIF, QUALNUM, LASTQUAL, and PICT in "Field value manipulation" on page 760.

The examples at the end of this section show the use of a WHERE clause for the CONVERSION command.

Examples of CONVERSION command syntax

Example 1

```
CONVERSION conv1 REPLCHAR((qual1,'a'))
```

Defines a conversion named conv1 of default type ACCESS NEWLIST that replaces the characters of the first qualifier with the character a. For a field value of xxx.yyy.zzz, conv1 changes it to aaa.yyy.zzz.

Example 2

```
CONVERSION TYPE=ACCESS conv2 REPLCHAR((qual1,'a'),(qual2,'b'))
  WHERE (class=dataset,qual(resource,1)='C2PACMON',qualnum(resource)=5)
```

Defines a conversion named conv2 of explicit type ACCESS NEWLIST that replaces the first qualifier in the field value by characters a and the second qualifier in the field value by characters b.

This conversion is completed for records where the value of the CLASS field is DATASET, the first qualifier of the RESOURCE field value is C2PACMON, and the number of qualifiers for the RESOURCE field is 5. For example, if the field value is c2pacmon.www.xxx.yyy.zzz, conv2 changes it to aaa.bbb.xxx.yyy.zzz.

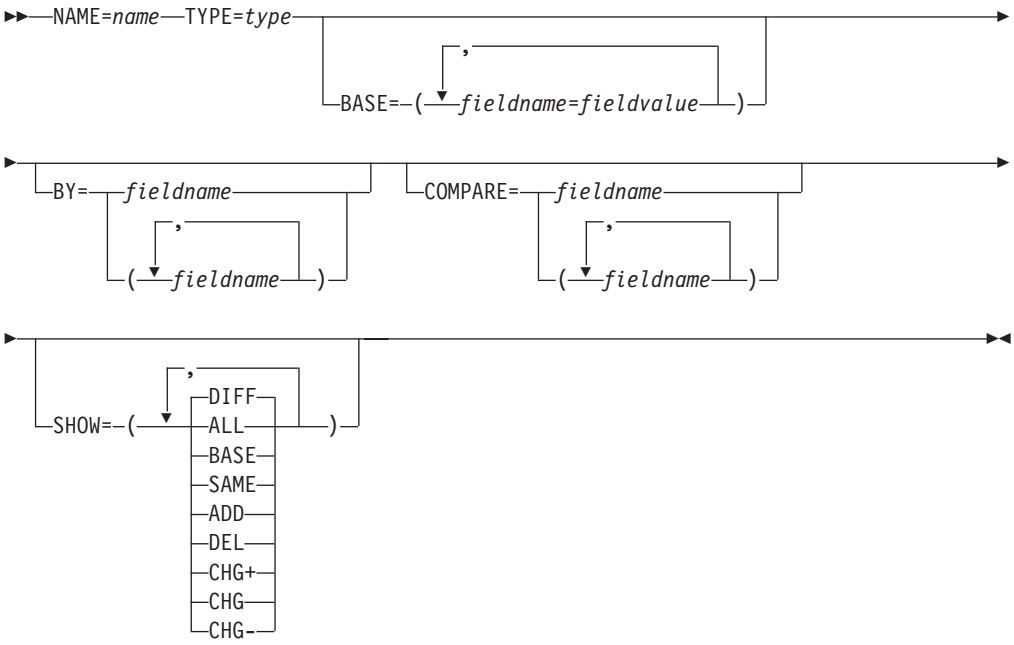
COMPAREOPT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The COMPAREOPT statement defines a set of comparison properties to be used by any NEWLIST that references it using the COMPAREOPT=name option. The COMPAREOPT statement specifies what is to be compared in a comparison process and what is to be shown in the output. For information about how compare processing works, see "Compare processing" on page 46.

The COMPAREOPT has the following syntax:

CompareOpt



The parameters available for the COMPAREOPT statement are described in the following sections.

NAME=

Specifies the name of this COMPAREOPT statement. The name is used to select this COMPAREOPT specification in a NEWLIST statement. This field is required. The name *DEFAULT* is a pre-defined compare specification that cannot be modified. It is established by the ALLOC FUNCTION=BASE option. See "ALLOCATE" on page 718.

The NAME parameter must be specified before the BASE parameter option.

TYPE=

This required field specifies the NEWLIST type to which this COMPAREOPT statement applies.

The TYPE parameter must be specified before the BY, BASE, and COMPARE parameters.

BASE=

Specifies the criteria to be used to locate the record that reflects the BASELINE. It is specified in the form of a SELECT clause appropriate for the NEWLIST type. If no base is specified, the lowest value present in the record collection is used. For more information, see "Compare processing" on page 46.

The value for the BASE parameter can also be set using the `ALLOC FUNCTION=BASE` specification. For details, see the FUNCTION parameter in "Explicit allocation mode" on page 720.

BY=

Specifies the key of the record to be used in the comparison process. No DEFINE variable names are supported here. Do not include any fields used in the BASE specification. If it does, each set of BY values contains only one record with a compare result value of either ADD or DEL. Many NEWLIST fields have a default set of BY variables. You can use `TYPE=FIELD` to obtain this default set.

COMPARE=

Specifies the fields to be used in the comparison process. No DEFINEd variables are supported here. Not all variables are supported. You can use `TYPE=FIELD` to determine which fields are supported.

SHOW=

Specifies the records to be included in the resulting display or report. A value of *ALL* is equivalent to all possible values. A value of *DIFF* represents a composite of `ADD`, `DEL`, `CHG`, `CHG+`, and `CHG-`. For an explanation of these values and other possible values, see "Defining variables for comparison results (COMPAREOPT)" on page 754.

Processing considerations

- If any of the BASE, BY, or COMPARE field names specifies the name of an unsupported field, an error message is issued. Then, after the parsing phase, the program stops. To prevent this problem, you often need to use the default values, or to list all the comparison fields that you are interested explicitly.
- For the BY= parameter, unsupported fields mainly include structured repeated fields.
- For the COMPARE= specification, unsupported fields include those fields that cannot reasonably be compared and represented in a report. Examples are repeated combination fields, like ACL and CONNECTS. Simple repeated fields are supported, although most of these do not provide useful information when used out-of-context, USERACS for example.
- You cannot specify lookup fields or defined variables for any of the BY or COMPARE field names.
- Although you can specify a field as both a compare field (COMPARE) and a record key (BY) field, this specification is not useful. The compare process result for this specification is *fields are equal*. Almost the inverse applies to specifying the same field as a compare field (COMPARE) and as part of the baseline key (BASE). In that case the outcome of the comparison process is BASE (for the baseline record) or one of the difference values for all other records.

COPY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•			

The COPY command generates RACF commands to copy the user or group profile including all attributes and all segment information that can be set by RACF commands. The connects are also copied, including all connect attributes except the connect OWNER, which is always set to the group. When you copy user- or group-specific profiles, all occurrences of the user or group are replaced by the target ID. User- or group-specific profiles are profiles with the user or group at a predefined qualifier in the profile key. If you supply a CKFREEZE file, IDCAMS commands are used to copy the corresponding catalog aliases.

Note: The REMOVE command is only supported if you have IBM Security zSecure Admin installed and enabled.

The COPY command does not issue any commands by itself. The generated RACF commands are written to the CKRCMD file. The commands in this file can also be generated as the result of the following commands: MOVE, REMOVE, VERIFY command or a PRINT DD=CKRCMD statement. If commands are being queued from the interface, then commands in CKRCMD can also be generated by overtyping, including the extra SETROPTS REFRESH commands. To complete the copy operations, verify and confirm the commands in the CKRCMD file, and then run them.

The COPY command generates the RACF commands for each complex/security database that has the model user defined. When the commands are run from the CKRCMD file, the operations can fail if the requisite profiles have disappeared. For example, if an existing profile to be copied refers to another profile that has been deleted, the copy operation fails. The failure occurs because RACF only checks validity at the time a profile is being added or modified and does not enforce referential integrity.

Some information cannot be copied by regular RACF commands. Most notably, these include a user's initial TSO command and the TSO User Profile Table, which are both options set by the TSO PROFILE command.

The COPY command syntax is similar to the syntax for the COPY and REMOVE commands. The COPY command is mutually exclusive with VERIFY PERMIT and VERIFY STC commands.

The keys and members of RACFVARS profiles are by default interpreted as users and groups when they match a valid user or group id, and they are managed accordingly, unless you specify the SUPPRESS MANAGERACFVARS command for the run. A discrete first qualifier in the key of a STARTED profile is only interpreted as a user ID when it matches the specification in the STUSER field in the STDATA segment.

You can specify the information to be copied using the COPY parameters described in “COPY parameter descriptions” on page 742. “Using the COPY command” on page 746 provides examples of using the COPY command and parameters.

When the COPY command runs, the resulting messages are similar to the messages generated by the MOVE and REMOVE commands except the COPY messages include *Copy* or *Replace* terms instead of *Delete* and *Remove*. The term *Replace* is used when a command has been generated to remove a permit to the original user/group in a new profile. It is also used when a command has been generated to replace a field in a new profile (OWNER, for example). The term *Copy* is used if a new permit has been added as a copy of a permit to the original user/group. The COPY messages can also include the phrase *Resource copying:* when referencing new catalog aliases.

COPY parameter descriptions

Use the following parameters to specify the user or group information to copy and the target and where it is to be copied. The order in which the parameters are specified is significant. For examples showing how to use the COPY command, see "Using the COPY command" on page 746.

PERMIT= *id* **TOUSER=***id2*
Generate commands that would add permits for user *id2* to all access lists containing permits for user or group *id*. In addition copies of all generic data set profiles starting with the user or group id are added. The scope of the command can be limited by using the SELECT QUAL= command.

PERMIT= *id* **TOGROUP=***id2*
Generate commands that would add permits for group *id2* to all access lists containing permits for user or group *id*. In addition copies of all generic data set profiles starting with the user or group *id* are added. The scope of the command can be limited by using the SELECT QUAL= command.

PERMIT= *id* **TOPERMIT=***id2*
Generate commands that would add permits for user or group *id2* to all access lists containing permits for user or group *id*. In addition copies of all generic data set profiles starting with the user or group *id* are added. The scope of the command can be limited by using the SELECT QUAL= command.

USER= *id* **TOUSER=***id2*
Generate commands to copy a user including its usrdata, segments, connects, permits, and the profiles used by that user only. This parameter does all processing of COPY PERMIT, and also generates RACF commands to create the user to its default group, connects it to the other groups, creates copies of all generic data set profiles starting with user ID, and creates copies of all general resource profiles or members with the user ID in functional positions in profile keys of the following classes:

- DATASET
- DLFCLASS
- INFOMAN
- JES: JESJOBS, JESSPOOL
- CICS: TCICSTRN, GCICSTRN, DCICSDCT, ECICSDCT, FCICSFCT, HCICSFCT, ACICSPCT, BCICSPCT, JCICJCT, KCICSJCT, MCICSPPT, NCICSPPT, PCICSPSB, QCICSPSB, SCICSTST, UCICSTST, CCICSCMD, VCICSCMD
- VM: VMMDISK, VMRDR, VMBATCH, VMCONECT, VMEVENT, VMXEVENT, VMCMD
- LFSCLASS
- SURROGAT
- PROPCNTL
- PTKTDATA

When copying a profile, permits and the OWNER and NOTIFY fields are also replaced if they contain the user ID to be replaced in the original profile. The scope of the command can be limited by using the SELECT QUAL= command as well as by the SUPPRESS ADDSD command. The connects to be defined can be regulated by the FROMGROUP and TOGROUP parameters. If FROMGROUP specifies a list of groups, the new user ID is not connected to any of these groups. If TOGROUP is specified, a connect with default attributes is added for that group. More than one COPY USER=*id* can be present for the same id to create a

set of user IDs with identical setup. COPY for an already defined user does not generate the CONNECT and ALTUSER commands by default. This prevents a user from inadvertently copying over an existing user ID. You can make a conscious decision to copy to a user ID that exists: by suppressing messages 535 and 536 (option **SE.0**), the commands will be generated even though the user exists.

GROUP= *id* **TOGROUP=***id2*
Generates commands to copy a group, including its segments, connects, permits, and the profiles solely used for that group. This parameter does all COPY PERMIT= processing and in addition it generates the RACF commands to add the group below the same superior group, create connects to the same users, create copies of all generic data set profiles starting with group, and create copies of all general resource profiles with the group in functional positions in profile keys of the following classes:

- DATASET
- DLFCLASS
- VM: VMMDISK, VMRDR, VMBATCH, VMCONECT, VMEVENT, VMXEVENT, VMCMD
- SURROGAT
- PROPCNTL
- PTKTDATA
- LFSCLASS
- JES: JESJOBS and JESSPOOL

When copying a profile, permits and OWNER fields are also replaced if they contain the group to be replaced in the original profile.

The following options can be used to modify the processing of the COPY USER=*id* TOUSER=*id2* command.

NEWDCEUUID('*new uuid***')**
NEWDCEUUID='*new uuid***'**
This parameter can be used with COPY USER=*id* TOUSER=*id2* command to set the DCE UUID for the new user ID. The string can be enclosed in single, double, or left quotation marks.

NEWDATA('*new installation data***')**
NEWDATA='*new installation data***'**
This parameter can be used with the COPY USER= TOUSER= command or COPY GROUP= TOGROUP= commands to set the installation data on the new ID. The string must be enclosed in single, double, or left quotations.

NEWDFLTGRP(*group***)**
NEWDFLTGRP=*group*
This parameter can be used with COPY USER= TOUSER= command to set the default group on the new user ID. It implies TOGROUP=group which means that a new default connect will be added if the original user ID was not connected to this group.

NEWKERBNAME('*new kerbname***')**
NEWKERBNAME='*new kerbname***'**
Use this parameter with the COPY USER= TOUSER= command to set the Kerberos principal name for the new user ID. The string can be enclosed in single, double, or left quotes. The Kerberos principal name is case sensitive and can contain internal blanks. You must specify a unique value for each user.

NEWNAME(*newname***)**
NEWNAME=*newname*
This parameter can be used with `COPY USER= TOUSER=` command to set the name on the new user ID. The string can be enclosed in single, double, or left quotation marks.

NEWOMVSGID(*new gid***)**
NEWOMVSGID=*new gid*
This parameter can be used with the `COPY USER= TOGROUP=` command to set the OMVS GID for the new group. The value of the new gid can be one of the following:

- A number (for example: 1234). The number that you specify is assigned as the gid for the new group.
- A number followed by the letter S (for example: 1234S). The value that you specify is assigned as the gid for the new group, using the SHARED keyword.(available in z/OS 1.4 or with APAR OW52135).
- The word AUTO. This value automatically assigns the new group a unique gid by using the AUTOGID command(available in z/OS 1.4 or with APAR OW52135).

If the NEWOMVSGID keyword is not present on the copy command, the value of the gid for the source group is used, and if running on z/OS 1.4 or later, the SHARED keyword is added.

NEWOMVSHOME('*new home directory***')**
NEWOMVSHOME='*new home directory***'**
This parameter can be used with `COPY USER= TOUSER=` command to set the OMVS path for the home directory for the new user ID. The string can be enclosed in single, double, or left quotation marks. The HOME path name can consist of any characters, including quotations.

NEWOMVSPROGRAM('*new shell command***')**
NEWOMVSPROGRAM='*new shell command***'**
This parameter can be used with `COPY USER= TOUSER=` command to set the OMVS path for the shell command for the new user ID. The string can be enclosed in single, double, or left quotation marks. The PROGRAM path name can consist of any characters, including quotations.

NEWOMVSUID(*new uid* **)**
NEWOMVSUID=*new uid*
This parameter can be used with `COPY USER= TOUSER=` command to set the OMVS UID for the new user ID. The value of *new uid* can be one of the following:

- A number (for example: 1234). The number that you specify is assigned as the uid for the new user.
- A number followed by the letter S (for example: 1234S). The value that you specify is assigned as the gid for the new group, using the SHARED keyword. (available in z/OS 1.4 or with APAR OW52135).
- The word AUTO. This value automatically assigns the new group a unique gid by using the AUTOGID command(available in z/OS 1.4 or with APAR OW52135).

If the NEWOMVSUID keyword is not present on the copy command, the value of the source users uid is used, and if running on z/OS 1.4 or higher, the SHARED keyword is added.

NEWOWNER(*owner***)**
NEWOWNER=*owner*
This parameter can be used with `COPY USER= TOUSER=` command to set the owner on the new user ID.

NEWPHRASE('*phrase***')**
NEWPHRASE= '*phrase***'**
Use the NEWPHRASE parameter to set the password phrase on the new user ID. The password phrase value is case-sensitive. When you specify the value, it is not echoed in the SYSPRINT. The following syntax rules apply to the value specified for phrase:

- Maximum length: 100 characters.
- Minimum length: nine characters if ICHPWX11 is present and 14 characters if ICHPWX11 is not present.
- Must not contain the user ID (as sequential uppercase or sequential lowercase characters).
- Must contain at least two alphabetic characters (A–Z, a–z).
- Must contain at least two non-alphabetic characters (numerics, punctuation, or special characters).
- Must not contain more than two consecutive characters that are identical.
- If a single quotation mark is intended to be part of the password phrase, you must use two single quotation marks together for each single quotation mark.

The NEWPHRASE parameter is mutually exclusive with the PROTECTED parameter.

NEWPASSWORD(*password***)**
This parameter can be used with `COPY USER= TOUSER=` command to set the password on the new user ID. The password is not echoed on SYSPRINT. It is mutually exclusive with the PROTECTED parameter.

NEWSNAME('*new sname***')**
NEWSNAME='*new sname***'**
This parameter can be used with `COPY USER= TOUSER=` command to set the Lotus Notes short name for the new user ID. The string can be enclosed in single, double, or left quotation marks. The `sname` is case sensitive and can contain internal blanks. You must specify a unique value for each user.

NEWUNAME('*new uname***')**
NEWUNAME='*new uname***'**
This parameter can be used with `COPY USER= TOUSER=` command to set the NDS user name for the new user ID. The string can be enclosed in single, double, or left quotation marks. The `uname` is case sensitive and can contain internal blanks. Make sure that this field has a unique value for each user.

FROMGROUP(*idlist***)**
FROMGROUP=*id*
FROMGROUP=(*idlist***)**
This option causes a user ID not to be connected to the groups specified in *idlist*, which can be a single group name, or a list of group names enclosed in parentheses and separated by commas. Multiple FROMGROUP parameters have the same effect as a list of groups. If a group happens to be the default group of a user, the default group is changed to one of the TOGROUP groups (if present, which one exactly is unpredictable), or another connect.

TOGROUP= *idlist*[5]
This option can be added to the `COPY USER=` command to indicate additional connects to be created. They are specified as *idlist*, which can be a single group name, or a list of group names enclosed in parentheses and separated by commas. Multiple TOGROUP parameters have the same effect as a list of groups. In addition, it can be used as an alternative default group if a FROMGROUP happens to be the default group of a user.

PROTECTED
This parameter can be used with `COPY USER= TOUSER=` command to protect the password on the new user ID. This means that the user ID has no password and cannot be used in logon procedures.

The PROTECTED parameter is mutually exclusive with the NEWPASSWORD and NEWPASSPHRASE parameters.

REVOKE
This option can be used on the `COPY USER=` command to revoke the user ID as well as performing the other actions on the COPY command.

Note: All parameters except NEWPASSWORD and NEWPHRASE can also be specified as `parm(value)` in addition to `parm=value`.

Using the COPY command

The following examples show the command syntax to use for various copy tasks such as copying a user or a group.

Copying permits

The following example generates commands to copy permits. The COPY PERMIT command adds a user SMITH on all access lists that contain user JONES, with the same access permitted as for user JONES, and creates generic data set profiles starting with SMITH for ones starting with JONES, to allow the same access to corresponding data sets.

```
copy permit=jones touser=smith
```

Copying permits selectively

The following example generates commands to copy permits for a specific user ID JONES to another user SMITH, and creates generic data sets profiles starting with SMITH for the ones starting with JONES, but only for profiles with MYAPP as their first qualifier.

5. Idlist is one or more ids separated by commas or blanks.

```
select qual=myapp
copy permit=jones touser=smith
```

Copy user

The following example generates commands to create a clone of user JONES, and call it SMITH.

```
copy user=jones touser=smith newname='JOHN SMITH'
```

If you omit the new name, the name is copied from JONES.

For details on controlling password-related information for the new user ID, see "COPY parameter descriptions" on page 742 the NEWPASSWORD, NEWPHRASE, and PROTECT parameter descriptions.

Copying user - leave revoked

The following example generates commands to clone a user ID JONES and call the clone SMITH, but revoke the new SMITH user ID.

```
copy user=jones touser=smith revoke
```

Copying a group

Generates commands to copy permits, connects, and group-specific profiles for a group OLDGRP to another group NEWGRP.

```
copy group=oldgrp togroup=newgrp
```

Copying a user without resource profiles

The following command example generates the commands to copy permits, connects, and user attributes for a user ID JONES to another user SMITH without copying the user-specific profiles.

```
copy user=jones touser=smith
suppress addsd
```

Copying a user to another group

```
copy user=jones touser=smith
fromgroup=oldgrp togroup=othergrp
```

The following example generates the commands to copy the permits, connects, user attributes, and user-specific profiles for the user ID JONES to the SMITH user ID and connects SMITH to a new group (OTHERGROUP) instead of the group that JONES was connected to (OLDGROUP).

In this case, the connect attributes of `SMITH/OTHERGRP` are the default, `AUTH(USE)`, instead of any attributes of `JONES/OLDGRP`.

Copying a user without catalog aliases

The preceding examples clone catalog aliases for which the sourceid is the HLQ. This example clones a user but does not create any catalog aliases.

```
copy user=jones touser=smith newname='JOHN SMITH'
suppress copyalias
```

Cloning multiple user IDs from a model user

The following example generates a set of user IDs from one model.

Important: Do not use a fixed algorithm for deriving new passwords.

```
copy user(coursem) touser(course1) newname('student 1'),
newpassword(student1)
```

```
copy user(coursem) touser(course2) newname('student 2'),
newpassword(ticpw2)

copy user(coursem) touser(course3) newname('student 3'),
newpassword(yapfstu3)

copy user(coursem) touser(course4) newname('student 4'),
newpassword(newpwst4)
```

DEBUG

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command is meant to diagnose problems in the operation of the program. With the exception of the following parameters, most of the DEBUG parameters are not documented in this manual. Use the DEBUG command when advised to do so by IBM Software Support.

This command is not supported in restricted mode, except for PERFORM, DICT, ACTION, CPIC, RESTRICT.

The DEBUG options that are documented are:

ABEND
Issues an immediate user abend 16 for the purpose of testing error recovery procedures and stops further processing.

ACTION
Prints the message CKR2829 to list the National Language Support decisions during processing of an action command under ISPF. This field also prints CKR2670 messages to document the substitution map being used by a FORALL command.

CPIC
This parameter no longer has meaning since CPI-C support has been removed from the program.

EMAIL
This option can be used to diagnose email address problems. It lists messages detailing the program's understanding of the email address passed in terms of phrase, local-part, and domain. It also lists the line length used for the email output.

FIELD
Gives detailed diagnostic information about the processing of fields from RACF profiles.

GUARD
Branches to an odd address (0C6 abend) within guarded code. This should not lead to a crash.

INDEX
This parameter requests debug output that lists which profiles are actually read from a RACF data set, and which profiles lookups are taking place. It can be used to debug query response time problems. This parameter is not supported in restricted mode.

LICENSE

This causes install, entitlement, and product enablement status to be listed in the SYSPRINT.

DEBUG LICENSE only has effect if it comes in the input before any CARLa constructs that need access to entitlement information for some reason (like a DEFINE before the first NEWLIST). Generally this means it is most effective when passed in the parameter string. For the ISPF interface, you can use the Preamble, see "SE.3 Setup - Preamble" on page 1654.

PERFORM
This parameter does the following:

- Requests debug output that details which NEWLIST / select can exploit the RACF data set index.
- Lists the initial key request queue.
- Can be used to debug query response time problems.
- Triggers the creation of CKR1698 messages in the `SYSPRINT`.

  These messages report elapsed and CPU time at various stages in the processing. They report both the delta since the previous CKR1698 (or start of program for the first message), and the total elapsed time since the program started. Information is more complete under ISPF, providing the status messages themselves in the `SYSPRINT` with record counts and other information. In batch mode, only the ISPF message number is listed without the message content.

This parameter is supported in restricted mode.

READALL
This parameter requests debug output concerning the tests for the CKR.READALL profile in the CKRSITE class.

RESTRICT
Prints message CKR2854 to list the TCB dirty bits and the module dirty bits of all modules in the Job Pack Queue to help in PADS debugging. This is also automatically activated by a 913 abend on CKFREEZE, CKRUNLIN, or a RACF database.

SEGMENT
This parameter requests debug output that shows where a user or group segment was found that could not be accurately assigned to the proper entity type. This may happen for OMVS segments that have only the field UID filled in.

SVC99
This debug option shows all debugging information for all SVC 99 (DYNALLOC) calls being done.

DEFAULT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command can be used to change defaults. They apply for the complete run.

OWNER= *id*
Select a different default ownership than SYS1 for non-data set profiles that have an undefined owner or an owner that is to be removed.

SYSTEM= *id*
SYST=*id*
SYS=*id*
Select system to use as viewpoint if only one system at a time is supported. This applies for instance to the REPORT AC1 command. complex simply is the one the default system has been assigned to. The default system and complex are listed in the SYSPRINT file in the CKR0615 message.

If the DEFAULT specification is omitted, an arbitrary system is selected from any CKFREEZEs present. However, if one of the CKFREEZE files applies to the current system, then this is used as the default system (if the DEFAULT specification was omitted).

DEFINE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The DEFINE command is used to define variables for several purposes.

- *Statistic variables* to be used with the (D)SUMMARY command.
- *Boolean variables* for use with the (D)SUMMARY, SORTLIST, LIST and DISPLAY commands, and non-RACF SELECT and EXCLUDE commands. There are two kinds of Boolean variables, BOOLEAN and TRUE; the type BOOLEAN is a summary statistic and cannot be part of a summary key, the type TRUE is a field and can be part of a summary key. The difference is only apparent on the (D)SUMMARY command.
- *Subselect variables* to list selected repeat group instances with the SORTLIST, LIST, and DISPLAY commands.
- *Field-based variables* to define a variable based on a field, but with a different layout or with conditions attached, for use with the (D)SUMMARY, SORTLIST, LIST and DISPLAY commands, and non-RACF SELECT and EXCLUDE commands.

If a variable is defined that has the same name as a built-in field, the defined variable is used in the SELECT and EXCLUDE output commands. Within a DEFINE command, the field on which a variable is defined is always the original field. The DEFINE command can be abbreviated to DEF.

Variables defined with a DEFINE command apply to one NEWLIST type unless TYPE=* is specified. TYPE=* is a multi-type define that results in the variables being defined being available in all NEWLIST types. Variables can have local scope (that is, become undefined at the next NEWLIST) or have global scope (that is, remain defined until overridden). To indicate the NEWLIST type to which the variable applies, the TYPE= parameter is used. If not used, the current NEWLIST type is used by default. (Before the first NEWLIST, type=RACF is implied.) The following table shows how the scope of a DEFINE is set:

Table 287. DEFINE Scope

Within a NEWLIST	Using TYPE=	Type	Scope
Yes	Yes	*	Global, Multi-type
No	No	RACF	Global
No	Yes	from TYPE	Global

Table 287. DEFINE Scope (continued)

Within a NEWLIST	Using TYPE=	Type	Scope
Yes	No	from NEWLIST	Local, unless first definition
Yes	Yes	from TYPE	Local, unless first definition

Variables that are defined can only be used in commands that are situated *after* the DEFINE and are within scope of the define. Since the first definition of a variable with a certain name and type always has a global scope, this means that the variable can be used in all commands beyond the DEFINE. When both a global and a local variable with the same name and type are in scope for a NEWLIST be aware that the local variable is used in all commands following the local DEFINE and the global variable is used in all commands preceding it.

The DEFINE command has the following basic syntax:

```
DEFINE
    [ TYPE=type ]
    [ HELPPANEL=panelname ]
    varname[(modifiers)]
    definition
    [ WHERE clause ]
```

The general *definition* syntax is

```
kind[specification]
```

TYPE

The TYPE=*type* parameter is optional. It defines to which NEWLIST type the definition applies. The default is that the definition applies to the current NEWLIST type (if in the scope of a NEWLIST), or RACF if the DEFINE is not in a NEWLIST scope.

To define a variable, `varname` for all NEWLIST types, use `TYPE=*`. Specifying `TYPE=*` can reduce some of the maintenance effort for defining statistical fields that are often used in multiple newlists. The use of TYPE=* is also called a *multi-type define* in contrast to a *global define* which refers to DEFINE statements specified outside the scope of a NEWLIST.

`TYPE=*` results in the `varname` being available in all NEWLIST types. Using `TYPE=*` can reduce some of the maintenance effort for defining statistical fields that are often used in multiple newlists. The use of `TYPE=*` is also called a multi-type define. The term global define is already in use for defines done outside the scope of a NEWLIST.

If the variable that is being defined exists, one of the definitions needs to be overridden or ignored. For `TYPE=*`, the most recent definition during parse of the CARLa input statements is used. This results in using different definitions for `varname` based on the sequence of define and use statements. The following considerations apply to `TYPE=*`:

- `TYPE=*` is only supported by the following `DEFINE` types: `COMPARE_RESULT`, `COMPARE_CHANGES`, `COUNT`, and `SUMCOUNT`.
- A `WHERE` clause is not supported by `TYPE=*` because select clauses are type-dependent.

HELPPANEL= *panel*

This indicates which help panel to use when field-level help is being requested. This parameter must be specified before the field name on the DEFINE and can be before or after the TYPE= keyword. If this help panel name is not specified,

it defaults to help for the field on which the DEFINE is based. If the specified or default field-specific help panel does not exist, it falls back to the help panel on the NEWLIST or OPTION statement appropriate for the current display level (HELPPANEL, DETAILHELPPANEL, or SUMHELPPANEL). If that is not specified, it defaults to the newlist help panel C2R&CKREREL.xx@0 where xx is the two letter NEWLIST type representation. The panel name specified may contain "&CKREREL." to be replaced with 2 or 3 depending on the ISPF level (2 for VM), but not in the first position.

varname
The *varname* parameter can be 1 to 24 characters long, can contain alphanumeric characters, underscores, and the national characters **#**, **$**, and **@**. The *varname* cannot start with number. National characters cannot be used for output in XML format. To avoid name clashes with predefined fields it is advisable to use two underscores as a prefix.

If a variable is defined that has the same name as a built-in field, the defined variable is used when the name is referred to in SORTLIST and in DISPLAY commands. If you define a variable with the same name as a built-in field, and then use that name as a target for a subsequent define, the built-in field is used, not the defined variable.

The optional modifiers for the DEFINE statement *varname* parameter are described in the following paragraphs:

modifiers
The output modifiers included after the variable are optional. They are described with the LIST command, see “LIST family of commands” on page 794.

kind
This defines the kind of variable. The variable can be AVG, AS, BOOLEAN, COUNT, FREQ, MAX, MIN, SUBSELECT, SUM, SUMCOUNT, or TRUE. The kinds of variables supported are documented in “Defining variables for a summary” on page 753 and “Defining variables for a SORTLIST/DISPLAY” on page 754. See these topics for more information.

specification
The *specification* extends the definition of the *kind* variable. The following syntax shows the supported combinations of *kind specification*:

```
{ {MIN|MAX|AVG|SUM}(field)
  | {COUNT|SUMCOUNT|FREQ|BOOLEAN}
  | {COUNT|SUMCOUNT|FREQ|BOOLEAN}(target variable)
  | {COMPARE_RESULT|COMPARE_CHANGES}
  | SUBSELECT field(subselect clause)
  | AS expression
  | TRUE
}
```

WHERE
The optional WHERE clause is an expression that is formed like a SELECT or EXCLUDE clause for the current NEWLIST type and uses the same fields, relationship operators, and so on. A WHERE clause is not supported for `DEFINE TYPE=*` because SELECT clauses are type-dependent.

If the WHERE clause evaluates to TRUE this means that a similar SELECT clause would have selected the record and the WHERE clause is effective. The effect of the WHERE clause depends on the variable type: a summary statistic is updated, a Boolean is set to ON, or a field-based variable is used.

If the WHERE clause evaluates to FALSE, a statistic is not updated, a Boolean is set to OFF, a subselect is not performed (all instances are skipped), or a field-based variable is missing.

For usage examples, see "Example: WHERE clause for summary statistics" on page 773.

Defining variables for a summary

You can define variables for use in a (D)SUMMARY command to collect statistics about a field, or to count occurrences. Table 288 shows the variable categories that can be defined.

Table 288. Variable categories that can be defined for the SUMMARY command

Kind	Category	Meaning
AVG AVERAGE	field	Average of the fields that are summarized.
BOOLEAN	occurrence	YES if any of the occurrences evaluates to YES, NO otherwise. The only type of variable name that is supported in parentheses behind BOOLEAN is a variable with a WHERE clause. The statistic tests whether the WHERE clause is true in at least one record.
COUNT	occurrence	Count of occurrences. The only type of variable name that is supported in parentheses behind COUNT is a variable with a WHERE clause. The statistic counts the records where the WHERE clause is true.
FREQ FREQUENCY	occurrence	Percentage that the condition clause evaluates to true among occurrences (when combined with a condition clause), or percentage of occurrences selected (without a condition clause).
MAX MAXIMUM	field	Maximum of fields summarized.
MIN MINIMUM	field	Minimum of fields summarized.
SUM	field	Sum of fields summarized.
SUMCOUNT	occurrence	Count of different cases summarized on the next lower level, *after* the lower-level thresholds have been applied. The only type of variable name that is supported in parentheses behind SUMCOUNT is a variable with a WHERE clause. The statistic counts the lower summary levels where the WHERE clause is true in at least one record.

The use of summary statistics and the optional WHERE clause is shown in the examples at the end of this section.

Usage notes

- The NOPROP and *threshold* output modifiers can be used on a (D)SUMMARY command.
- An overriding length also has a special meaning in summaries. See "Modifying output length" on page 797 for more details.
- All variables for SORTLIST and DISPLAY as listed in the next section can be used on the (D)SUMMARY command as well; these act as summary key fields. In particular, TRUE can be used to split records for which the variable is true from those records for which it is false on the summary level, as opposed to BOOLEAN, which merely observes if any value true occurs in the summary category.

Defining variables for a SORTLIST/DISPLAY

You can define variables for use in a SORTLIST/DISPLAY to manipulate the presence, appearance, or contents of (part) of a field.

Table 289. SORTLIST/DISPLAY defined variables

Kind	Category	Meaning
AS	key	Copy of the original field. Useful for BUNDLEBY, to have a set of default overrides (length, format, and so on), to apply field value manipulations, or to only show a field subject to a specific WHERE clause.
SUBSELECT	key	Extract of a repeated field, filtered on the entry level according to a (possibly composite) SUBSELECT clause.
TRUE	key	TRUE, unless its WHERE clause evaluates to false.

Note: You can also use the summary statistic BOOLEAN in SORTLIST or DISPLAY commands. Specifying BOOLEAN is functionally equivalent to TRUE.

More information is available in the topics "Subselect clauses" on page 755, "Field-based defines" on page 760, and "Field value manipulation" on page 760, and in the example topics in this section.

Defining variables for comparison results (COMPAREOPT)

You can define the `COMPARE_RESULT` and `COMPARE_CHANGES` variables to store the results of a comparison process. See "Compare processing" on page 46 for information about the comparison process.

COMPARE_RESULT
Contains the results of the comparison process. Table 290 lists the possible values for the `COMPARE_RESULT` field.

Table 290. COMPARE_RESULT field - possible values

Field	Value
ADD	The baseline record corresponding to the current record is missing.
DEL	The baseline record is present, and the corresponding record in at least one other input source file is absent.
CHG+	Both the current record and the baseline record are present. At least one of the compare fields was found to be different. All changed compare fields support the same level or an increased level of security compliance. At least one of field changes represents an improvement.

Table 290. COMPARE_RESULT field - possible values (continued)

Field	Value
CHG-	Both the current record and the baseline record are present. At least one of the compare fields was found to be different, and at least one of the changed compare fields results in a decreased level of security compliance.
CHG	Both the current record and the baseline record are present. One of the compare fields was found to be different. None of the changed compare fields has an impact on the security compliance level.
SAME	Both the current and the baseline record are present, and all compare fields are identical. This does not necessarily mean that the entire two records are identical. They will differ in the key, and possibly some of the ignore fields.
BASE	The record reflects the baseline record. If the corresponding record in at least one other input source file is absent, the BASE value is suppressed by the DEL value.
MISSING	The current NEWLIST is not the result of a comparison operation. Instead of failing the entire process, the value is missing to reflect that no comparison result is available.

COMPARE_CHANGES

Contains the changes detected during the comparison process. The COMPARE_CHANGES field contains changed fields only. For each field the following values are included: *fieldname*, *compliance direction*, *baseline value*, *changed value*. The COMPARE_CHANGES field is in itself a repeated combination field.

Note: Use the SORTLIST or DISPLAY commands to include the comparison results stored in the COMPARE_CHANGES field in a printed report or display. You cannot use the SUMMARY of DSUMMARY commands to list these results.

The default format, CMPCHG4 formats the result in the form of quadruplets (*fieldname*, *compliance direction*, *baseline value*, *changed value*). If the fieldname is that of a repeated field, the *fieldname* is repeated as often as necessary to list different values. In this situation, the baseline value and the changed value shown on any single line need not be related in any way. Instead the repeat group entries are presented in an unpredictable sequence, as shown in the following example.

```
Fieldname       C Value-1                       Value-2
DFLTGRP           A                             C
CGGRPNM           A                             G
CGGRPNM           B                             E
CGGRPNM                                         F
```

The COMPARE_CHANGES field is sorted on the fieldname, which is in character format. If the field names are the same, they are sorted on the internal value of Value-1, and so on.

The sort order cannot be changed by the SORT modifier or DESCENDING.

For additional information about output formats, see “COMPARE processing output formats: Formatting COMPARE_CHANGES results” on page 829.

Subselect clauses

A subselect clause can be used to display only some entries from a repeated field. For example, you can use a subselect clause to display only those access list entries

with UPDATE access or higher. The subselect clause is most useful when the repeat group has many instances, of which only a few are of interest.

Only the ACL, CONNECTS, CUSTOM_DATA, and USR fields can be used for a subselect clause. Only the subselect CUSTOM_DATA and USR can be used on a LIST command. All subselect variables can be used on SORTLIST and DISPLAY commands. The EXPLODE, RESOLVE, EFFECTIVE, and TRUST modifiers can be used with the subselect ACL.

A subselect clause is like a SELECT, EXCLUDE, or WHERE clause in that it allows the following selection constructs: string match, pattern match, substring match, flag values, date values, authority level match, and access level match. Most tests can specify a single value or a list of values. However, a subselect clause tests on fields that occur within a single repeat group entry: The entire subselect clause is evaluated against each repeat group entry in isolation, so that, an AND condition matches only if there is an entry for which both of its parts are true simultaneously. The fields and subfields that can be used in a subselect clause are different from the fields that can be used in a SELECT statement. The subselect fields are described in Table 291.

Note: If a DEFINE ... SUBSELECT statement also contains a WHERE clause, the WHERE clause follows the normal rules for SELECT statements, not the rules for subselect clauses.

Some CUSTOM_DATA, ACL, and USR subselect clauses can also be used directly on the SELECT and EXCLUDE commands. See "SELECT/EXCLUDE ACL(...)" on page 890, "SELECT/EXCLUDE CUSTOM_DATA(...)" on page 890 and "SELECT USR(...)" on page 892.

Table 291 lists the fields that can be used with subselect ACL. The sample output following the table shows the ACL columns referenced in the table.

Table 291. ACL subselect - available fields

Field	Type	Meaning
ACCESS	access level	Access level as shown in the '*Access*' column. Defined for all repeat group entries.
GROUP	string	Group ID on an access list. For a normal (not exploded or resolved) access list, this is the ID as shown in the **ACL** *id* column, where the **User** column displays -group-. This field is not defined for those entries where the ACL ID is a user or is undefined.
ID	string	ID on an access list. This is the unexploded and unresolved ID, as shown in the **ACL** *id* column. This field is defined for all repeat group entries.
USER	string	User ID on an access list. For an exploded or resolved access list, this is the id as shown in the left column (**User**). This field is not defined for those entries where the ACL ID is a group or undefined.
WHENCLASS **WHENCLAS**	string	Class name used in a conditional access list. Only exists for those repeat group entries that have a conditional access list. Shown as part of the **When** column.

Table 291. ACL subselect - available fields (continued)

Field	Type	Meaning
WHENPROF **WHENPROFILE**	string	Profile or program name used in a conditional access list. This entry only exists for those repeat group entries that have a conditional access list. Shown as part of the **When** column.

Since ID acts on the unresolved and unexploded access list, it cannot be used to select on operations access. To only view operations access–including group operations access–, specify a subselect on ACCESS=ALTER-O.

The following sample output shows ACL fields and columns.

```
newlist
 s key=sysappl.cnracf.**
 sortlist key(20) acl(sort)
Profile key          User     Access  ACL id   When
SYSAPPL.CNRACF.**    -group-  READ    C##ACONF
                     -group-  READ    C##ARACF
                     -group-  READ    SYSBASE
                     -group-  READ    SYSSECUR
                     C##AINT  READ    C##AINT  PROGRAM  CNRACF
                     R##BDAG  UPDATE  R##BDAG  PROGRAM  CNRACF
                     R##PBRP  READ    R##PBRP
                     R##PROB  ALTER   R##PROB
                     R##PSEC  UPDATE  R##PSEC
                     R##PTST  READ    R##PTST  PROGRAM  CNRACF
```

Table 292 lists the fields that can be used with subselect CUSTOM_DATA.

Table 292. CUSTOM_DATA subselect - available fields

Field	Type	Meaning
CSKEY	String	Name of custom field
CSTYPE	Custom field type	The type of the custom field. Possible values are as follows: • Char • Num • Hex • Flag
CSVALUE	Character string, number, hexadecimal string, or flag	The value of the custom field. Because the CSVALUE field value is always handled as characters, you are likely to use a hex notation for the comparison value: For a hex string, you can use hexvalX. For example, for a numeric value of 255 you can use FFX and for flag fields you can use 80X to select true. Character fields can be selected in the normal manner.

The following sample output shows the fields in the CUSTOM_DATA repeat group. For the SORTLIST command, the individual fields in the CUSTOM_DATA group are shown because they most clearly illustrate the three fields available for the subselect clause. However, the default formatting for the CSVALUE field is CHAR, which means that for NUM, HEX and FLAG type fields, the value shown would consist of

non-printable characters. Instead of non-printable characters, the following example uses HEX format. This is also the only value that can consistently be used in the subselect CUSTOM_DATA for CSVALUE.

The following sample output shows the fields in the CUSTOM_DATA repeat group. The ouput is sent to separate fields in the group because there is no field that contains all columns.

```
 newlist type=racf
 select key=crmbsg1 class=user segment=csdata
 sortlist cskey cstype csvalue(hex)

Fldname  Type Custom field data
PHONE    CHAR F1F2F360F1F1F2F9F3F1F2
EMAIL    CHAR 8594979396A885857C85A781949793854B839694
EMPLNO   NUM  F5F2F7F7F1F1
DEPT     CHAR C6D6E4E3D1C5E2
```

An alternative method to display the same information would be to use the special output format CSVALUE for the CUSTOM_DATA field.

```
newlist type=racf
 select key=crmbsg1 class=user segment=csdata
 sortlist cskey cstype custom_data(csvalue)

Fldname  Type Custom field data
PHONE    CHAR 123-1129312
EMAIL    CHAR employee@example.com
EMPLNO   NUM  527711
DEPT     CHAR FINANCE
```

In most situations, a subselect for CUSTOM_DATA can effectively be replaced by a select and sortlist/display on the csname as shown in the following example.

```
newlist type=racf
 select key=crmbsg1 class=user segment=csdata EMPLNO=527711
 sortlist key emplno(8) dept

Profile  Emplno  Dept
USER123  527711  FINANCE
```

The following table lists the fields that can be used with subselect CONNECTS.

Table 293. CONNECTS subselect - available fields

Field	Type	Meaning
GROUP	string	Group in a connect instance. For a CONNECTS instance that is part of a group profile, this is the profile key; for a CONNECTS instance that is part of a user profile, this is a group the user is connected to, as listed in the "User/Grp" column.
GRPADSP	flag	Group-ADSP attribute, as listed in the "AG" column.
GRPAUD	flag	Group-auditor attribute, as listed in the "SOA" column.
GRPAUTH	connect authority	The connect authority (JOIN, CONNECT, CREATE, USE), as listed in the "Auth" column.
GRPGRPACC	flag	Group-grpacc attribute, as listed in the "AG" column.

Table 293. CONNECTS subselect - available fields (continued)

Field	Type	Meaning
GRPOPER	flag	Group-operations attribute, as listed in the "SOA" column.
GRPRESUMEDT	date	Connect-resume date, as listed in the Resumedt column.
GRPREVOKE	flag	Indicates whether the connect is revoked, using the unload date as a reference. Listed in the 'R' column.
GRPREVOKEDT	date	Connect-revoke date, as listed in the *Revokedt* column.
GRPSPEC	flag	Group-special attribute, as listed in the "SOA" column.
GRPUACC	access level	Group-UACC, as listed in the "UACC" column.
USER	string	User in a connect instance. For a CONNECTS instance that is part of a user profile, this is the profile key; for a CONNECTS instance that is part of a group profile, this is one of the users connected to the group, as listed in the "User/Grp" column.

The following sample output shows the CONNECTS field and its columns referenced in Table 293 on page 758.

```
newlist type=racf
 select key=ibmuser class=user
 sortlist connects
User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt

OMVGRP   USE              NONE
SYSCTLG  JOIN    R        READ
SYS1     JOIN      S      READ
VSAMDSET JOIN             READ    01 Jan 1996
```

Table 294 lists the fields that can be used with subselect USR. For more information about the USR field and its use by CKGRACF, and possible values of USR fields values referenced in Table 294, see Chapter 13, “SELECT/LIST Fields,” on page 953.

Table 294. USR subselect - available fields

Field	Type	Meaning
CKGAUTHOR	char	Requesting user of a queued command, if the USR field is a CKGRACF queued command; undefined otherwise.
CKGCHGDATE	date	Last change date of a queued command. if the USR field is a CKGRACF queued command; undefined otherwise.
CKGMULTI	char	Multiple-authority setting, if the USR field is a CKGRACF multiple-authority setting; undefined otherwise.
CKGREQUEST	date	Request date of a queued command. if the USR field is a CKGRACF queued command; undefined otherwise.

Table 294. USR subselect - available fields (continued)

Field	Type	Meaning
CKGSCHED CKGSCHEDULE	char	Schedule name, if the USR field is a CKGRACF scheduled revoke/resume action; undefined otherwise.
CKGSTATUS	char	Status of a queued command, if the USR field is a CKGRACF queued command; undefined otherwise.
USRDATA	char	Contents/value of the USR field.
USRFLG	flag	Flag in the USR field. You can either specify a hexadecimal value, or a bitmask.
USRNM	char	Index of the USR field.

Field-based defines

A field-based define is a definition where a variable is defined as another field. In its simplest form, the variable behaves exactly as the original field. You can add an overriding length, format, or header to get a new variable that behaves like the original field, but has a different layout or header. Finally, you can use any field value manipulation function such as `SUBSTRING` or `LOOKUP` that uses the original field as its source, and puts the result in the variable. (See "Field value manipulation") A field-based define uses the `DEFINE AS` command syntax, as follows:

```
define usdate(8,usdate) as date
define logged(hdr$blank,6,'Logged') as uaudit
define dflt_owner as dfltgrp:owner
```

A variable so defined can be used in SORTLIST, DISPLAY, and SUMMARY commands. These variables can also be used in SELECT/EXCLUDE statements. In the preceding examples, USDATE would be a useful shorthand if your reports always contain DATE(8,USDATE). Similarly, oft-repeated expression using look ups can best be written as defined variables.

Field value manipulation

In CARLa several functions for field value manipulation are available. These functions are designed to allow selection and reporting on only parts of a field, or on values based on, but not containing the field value (indirect references). These functions include the following:

CONVERT

When a character format field contains a date or number, normal processing always processes the field value as a string of characters. However, sometimes it is useful to process dates and numbers as values rather than strings. For example, if you have a character string that has date and time information, you might want to process the date and time parts of the string separately. The product provides the `CONVERT` function for this purpose.

The `CONVERT` function has the following syntax:

```
CONVERT(field, input format, internal format)
```

If a default internal format has been specified, you can use the following syntax:

```
CONVERT(field, input format)
```

The input format specifies the way the character format field currently contains the data. For example, the field might be a human-readable decimal field, or a packed-decimal field. The program uses the internal format to determine the correct selection and sort procedures for the data. An internal format also corresponds to a default output format.

The following list provides the input formats, the internal formats they can be converted to, and the default output format for printing the internally formatted field.

DATETIME (default)
In this input format, both the date and the time part of the string are in a sortable form. This format can be printed with most date and time formats. The supported format for date values can be found in "Date fields" on page 903.

The following internal formats are available to convert this format:

- DATE

  The date part of the field only. A value in this format field can be printed with the output formats ACF2DATE, DATE (default), JULDATE, USDATE, $DATE.
- SMFTIME

  The time part of the field only. A value of this format can be printed with the SMFTIME output format only. The SMFTIME output format is the default format.
- WEEKDAY

  The day of the week. A value of this format can be printed with the WEEKDAY output format only. The WEEKDAY output format is the default format.

The following processing rules apply to this format:

- The time is expected in the following format: hh:mm:ss:cc format. Hours and centiseconds can also be a single digit; seconds and centiseconds are optional. Instead of the colon (:), any single, non-space, non-digit separator can be used.
- Any text following the DATETIME specification is ignored.

DECIMAL
This input format is a human readable decimal integer, containing no commas or dots. The default internal format is DECIMAL, which is a standard numeric field that can be printed with the output formats DEC (default), DEC$BLANK, DEC$NO, and NUM.

PACKED
This input format is a packed decimal field as defined in the z/OS Principals of Operations. The default internal format is DECIMAL which is a standard numeric field. This internal format can be printed with the output formats DEC (default), DEC$BLANK, DEC$NO, and NUM.

SMFTIMESTAMP
This input format is the full time stamp as SMF stores it. This value can be printed with most date and time formats.

INTERNALDATETIME
This input format is the zSecure internal representation of the date and time. Using this format, you can convert a field defined as DATETIME into one of the following internal formats. The possible internal formats are as follows:

DATE
The date part of the field. This field can be printed with the output formats ACF2DATE, DATE (default), JULDATE, USDATE, $DATE.

SMFTIME
The time part of the field. This internal format can be printed with the SMFTIME output format only. The SMFTIME output format is the default format.

SMFTIMESTAMP
The date and time can be printed in SMF time stamp format.

WEEKDAY
The day of the week. This internal format can be printed with the WEEKDAY output format only. The WEEKDAY output format is the default format.

The following example shows the code to convert the input field to internaldatetime format for internal processing to be printed in the SMFTIMESTAMP format.

```
def type=svc mth("Mth",month,3)
convert(collect_datetime,internaldatetime,SMFTIMESTAMP)
```

LASTQUAL
Refers to the last qualifier in a field value. If the field value is aaa.bbb.ccc, the last qualifier is ccc. The syntax is LASTQUAL(*field*), where *field* is the field name.

PARSE
A particular section of a field, recognizable by unique identifiers before and after it, can be found with the PARSE operation. It has the following syntax:

```
PARSE(field, start separator[, end separator])
```

The *field* specified must have a character format. The *start separator* is the text right before the section wanted. The *end separator* is the text after the section wanted. For example, assume a field named DATA containing several items of information about a person: the name, function, and department. It is structured as follows:

```
Name: Doe, J.; Function: programmer; Dept: Data Processing;
```

or

```
Function: programmer; Dept: Data Processing; Name: Doe, J.;
```

```
PARSE(DATA,'Name: ',';')
```

will contain Doe, J.

If the start separator occurs more than once in the field processed, the first occurrence is used to calculate the field value to be returned. If the end separator is omitted, the returned value consists of all characters after the start separator to the end of the field.

PICT
Defines the character type of each character in the field value. The maximum supported field value length is 256 characters. The function returns a character string where each character represents the character type in the original field value. The possible types are:

- @ - represents an alphabetic character (A-Z, a-z)
- # - represents a number character ((0-9)
- $ - represents a punctuation character

- <space> represents a space character
- .(dot) represents all other characters

QUALIF
An index number from 1 to 123 that represents a qualifier segment of a field value. The syntax is QUALIF(field,index) where field is a name of a NEWLIST type in the form TYPE=*type*. The index is a number that represents the position of the qualifier segment in the name. If the field value is aaa.bbb.ccc, the index number 1 represents aaa.

QUALNUM
Calculates the number of qualifiers in the field value. The syntax is QUALNUM(field).

SUBSTRING, SUBSTR
Substrings can be generated from character fields using the SUBSTRING operation. The substring can have the following following formats:

- SUBSTRING(*field*,*startpos*,*length*)
- SUBSTRING(*field*,*startpos*:*endpos*)
- SUBSTRING(*field*,*startpos*)

The *field* specified must have a character format. The *startpos* is the start position where the substring of the field may start; the first character in the field has position 1. You can specify a *length* or an *endpos*. If you specify a length, it must be at least 1. If you specify an *endpos*, it must be equal to, or greater than, the *startpos*. If neither *length* or *endpos* are specified, the substring continues until the end of the field.

For example, consider a site that has defined the user IDs in the format DDGGNN, where DD is the department, GG the workgroup, and NN the user number in the group. The department can be specified as either SUBSTRING(USER,1,2) or SUBSTRING(USER,1:2). The group can be specified as SUBSTRING(USER,3,2) (using a *length*) or SUBSTRING(USER,3:4) (using an *endpos*).

On an ISPF display, variables defined as substrings with an output format of CHAR or ASIS are modifiable if the source field was modifiable. Multiple substrings may be on the display at the same time. They may even overlap, but any actual updates may not conflict with any of the other places on the screen where the same information is being displayed. Multiple substrings of one repeat group field may only be present on the same line of the detail display.

WORD
A particular word can be found in a character field with the WORD operation. This has the following syntax:

```
WORD(field,number[,delimiter(s)])
```

The *field* specified must have a character format. The *number* is the number of the word wanted (that is, the second word in the sentence for *number*=2). The delimiter can be a single character, possibly between quotations (necessary if you want to specify a comma or another type of quotation), or a string of up to 40 characters. Each occurrence of (one of the) character(s) you specified will indicate the start of the next word in the sentence. If you omit the delimiter, the words are separated by *one or more* blanks and blanks occurring at the start of the record will be skipped. When a delimiter is followed immediately by a quotation (either single, left or back quotation), the scan will first search for the balancing quotation and only the first delimiter thereafter will start the next word. If that delimiter immediately follows the balancing quotation (for

example, the result is a properly quoted string without further suffix), the quotations are stripped off. Otherwise, the quotations are left in place.

Some examples:

WORD(field,n) returns the nth blank delimited word, so:

```
field = "    one two   three 'four and five'"
```

results in:

```
WORD(field,1) = "one"
WORD(field,2) = "two"
WORD(field,3) = "three"
WORD(field,4) = "four and five"
WORD(field,5) = ""
```

WORD(field,n,delimiter) returns the nth token from the text string, where each occurrence of the delimiter signals the end of a token, so:

```
field = ";;one two; three;'four;five' "
```

results in:

```
WORD(field,1,';') = ""
WORD(field,2,';') = ""
WORD(field,3,';') = "one two"
WORD(field,4,';') = " three"
WORD(field,5,';') = "four;five"
WORD(field,6,';') = ""
```

Combining the functions

All the functions mentioned above can be combined to create complex expressions. If a field has been divided by semicolons and in the third part both a price and a comment are present in a random order, you could specify the price as follows:

```
PARSE(WORD(field,3,';'),'$',' ')
```

Taking just the dollar part, and storing it as an integer would be:

```
CONVERT(PARSE(WORD(field,3,';'),'$','.'),DECIMAL)
```

The email address of the salesman, whose LID or user ID is in the second part of the field would be

```
WORD(field,2,';'):EMAIL.USER.ADDRESS
```

Indirect reference or lookup

An indirect reference or lookup is the action of retrieving a different field from a database, based on the value of a base field. The general syntax for this is:

```
[basefield]:lookup-specification[:lookup-specification ...]
```

So an optional base field specification, followed by one or more levels of lookup. If the base field is omitted, we call that an object property lookup or implicit lookup operation. If the base field is present, we call it an explicit lookup operation and it can be an ID lookup, CLASS property lookup, SYSTEM property lookup, or a `deftype` lookup. If more than one lookup operator is present, the operation is known as a multi-level lookup. The lookup specification itself can contain one, two, or three qualifiers separated by a dot:

```
targetfield | type.targetfield | type.keyfield.targetfield
```

There is a difference between lookup in a SELECT or EXCLUDE statement and lookups in a LIST family command. For a SELECT type lookup to work, the data must be read into the program before the SELECT is executed. For a LIST family lookup this prerequisite does not apply. For DEFTYPE lookups, zSecure

can automatically determine the most optimal point where to read the data. However, this automation is not supported if a newlist of type A does a lookup to newlist type B in the SELECT statement, and a type B SELECT statement does a lookup to type A.

You can specify the following types of indirect references or lookups: Object property lookup, ID lookup, CLASS property lookup, SYSTEM property lookup, and deftype lookup.

Object property lookup

Lookup to request properties of a (security-related) object, written as

```
:targetfield
```

Object property lookups are currently only supported from the following NEWLIST types: SMF, RACF, TRUSTED, and REPORT_SCOPE. The target field will be retrieved from the security database. The security database (RACF) is determined automatically based on the available information, in CKFREEZE files for example. In anticipation of future versions, you can specify RACF as a target NEWLIST type in an object property lookup. However, this specification is currently ignored. For RACF systems, the key linking the target field to the source object consists of the combination of the complex, class, and RACF profile covering the resource. The target field can only be an existing field in the target database. Currently, if the target field specification is ambiguous (for example, present in multiple segments), the field value that is shown is not predictable. Defined variables are not supported.

Example object property lookup (RACF)

```
newlist type=smf
  select exists(profile)
  display resource :instdata
  dsummary class * profile
```

Example cross-segment object property lookup (RACF)

```
newlist type=racf
  s class=dataset segment=dfp
  display key complex :instdata
  dsummary resowner
```

Example object property lookup (RACF)

```
newlist type=report_scope
  report scope=ibmuser
  display key(firstonly) complex :racf.instdata
  dsummary via
```

ID lookup

The ID lookup is a lookup where the base field is interpreted as a user or group, and the target field is retrieved from that user or group. Use the following code to specify the base and target field values for the lookup:

```
basefield:targetfield
```

ID lookups are supported from all NEWLIST types. The target field is retrieved from the security database. The security database (RACF) is determined automatically, based on the available information in CKFREEZE files for example. Here, the key (source) of the lookup is a user ID or group ID. That is, the value of the base field padded to 8 characters is used to look up a user or group in the same complex as the record. The target field cannot be a variable. Currently, if the target field specification is ambiguous (for example, present in multiple segments), the field value that is shown is

not predictable. The id lookup can be repeated to create a multi-level lookup. It can also be added to extend any of the other lookup types to create a multi-level lookup.

Example id lookup (RACF)

```
newlist type=racf
  s  c=group s=base
  d key(8) supgroup owner owner:name owner:instdata
```

Example multi-level id lookup (RACF)

```
newlist type=racf
  s c=dataset s=base
  d class key owner owner:owner owner:owner:instdata
```

CLASS property lookup

The CLASS property lookup is an explicit lookup where the value for the base field is interpreted as a class name and an arbitrary class property can be used as the lookup result. This is done by specifying lookup target NEWLIST type CLASS and target NEWLIST key field CLASS. Use the following syntax to specify the base and target field values for a CLASS property lookup:

```
basefield:type.keyfield.targetfield
```

For instance to see whether a CLASS used in the past is now inactive, you could specify:

```
newlist type=smf
  select class:class.class.active=no
```

The CLASS properties are taken from the default system for the complex that the record belongs to, not necessarily from the system the record pertains to; typically, the system is the same for both. The CLASS property lookup is supported for the following NEWLIST types: RACF, TRUSTED, ACCESS, RACF_ACCESS, SMF, ROUTER, R_SCOPE, or R_PROFILE.

SYSTEM property lookup

The SYSTEM property lookup is an explicit lookup where the value for the base field is interpreted as an SMF ID, generally the CARLa SYSTEM field within the current complex and version. This is done by specifying lookup target NEWLIST type SYSTEM and target NEWLIST key field SYSTEM. An arbitrary non-repeating class property can be used. Use the following syntax to specify the base and target field values for the SYSTEM property lookup:

```
basefield:type.keyfield.targetfield
```

For example to select SMF records from RACF systems based on the &SYSCLONE system variable:

```
newlist type=smf
  select system:system.system.sysclone='01'
```

The SYSTEM property lookup is supported for the following NEWLIST types: ACCESS, CONSOLE, DYNEXIT, EXIT, IP_AUTOLOG, IP_INTERFACE, IP_NETACCESS, IP_PORT, IP_ROUTE, IP_RULE, IP_STACK, IP_VIPA, MOUNT, PPT, R_AC1, R_PADS, R_STC, RRSFNODE, SENSDSN, SMF, TRUSTED, and UNIX.

deftype lookup

This a lookup to a NEWLIST type define via the DEFTYPE command. All qualifiers in the lookup specification must be spelled out. The syntax is:

```
basefield:type.keyfield.targetfield
```

This requests an indirect reference to a database defined with DEFTYPE. Both the key field and the target field can be variables. The value of the base field in the source record is used as key field to locate the value of the target field. See the <deftype> field description for an example (on page 767).

For multi-level lookups, the lookups beyond the first one are by definition explicit lookups (either an ID lookup, or a deftype lookup), The base field specified must have a character format. No other limitations apply. Most fields are supported as a target field, except that the lookup returns only one value for a repeated field. Which value of a repeated field (the first, the last, or an arbitrary one) will be returned is unpredictable. The current selection of the returned value in a repeat group is not an intended interface. The NEWLIST types supported are:

RACF
Object Property Lookups retrieve information from the profile covering the resource object in the source NEWLIST type. ID Lookups treat the base field as a user ID or groupid and retrieve information from the user or group profile. Most fields of the target profiles are supported. For repeat group fields, only one value will be returned. Which repeat group entry will be used is unpredictable.

<deftype>
Indirect references are possible to any field of databases defined with the DEFTYPE command. The *newlist* type is the type specified on the DEFTYPE command, the *keyfield* is the defined field that should contain the value that corresponds to the value in the *basefield* and the *targetfield* is the defined field that contains the value referenced.

For example, a database has been allocated that contains two fields: the or user ID and the email address of that person. It has been defined with DEFTYPE TYPE=EMAIL and the two fields are defined as USER and ADDRESS. To report on the address of the users in the SMFUSERID field the specification would then be:

```
SMFUSERID:EMAIL.USER.ADDRESS
```

The lookup is performed without case translation. Consequently, the lookup value must match the case of the key-values present in the external lookup file. As most fields are uppercase, it is a good idea to use uppercase key-values for the email address lookup.

Defining fields in SMF records

In CARLa several functions for the retrieval of fields from an SMF record are available. These functions are the following:

RACF_SECTION
The RACF_SECTION function retrieves values described by a RACF relocate section within the SMF record. This is a possibly repeated section available only in RACF processing records (SMF 80, 81 and 83). Each section type is indicated by a number in the range 1 to 65535. The RACF_SECTION function has the following syntax: RACF_SECTION(*code*) or RACF_SECTION(*code,offset within section,length*). All values are in decimal; offset 0 indicates the start of the section. The version with one parameter uses the whole of the repeated section; the other version uses a specific part of the section. When used, the RACF_SECTION reads one value from the SMF record for each relocate section

in the record (it will not read beyond the end of the SMF record). RACF relocate sections are documented in the "Security Server RACF Macros and Interfaces" manual.

For example, the data set level field in a RACF processing record is described by relocate section 5. You can define this field using the following construction:

```
define type=SMF dsnlevel(3,dec) as racf_section(5)
newlist type=SMF
select dsnlevel>1
sortlist date time dataset dsnlevel
```

SMF_FIELD

The SMF_FIELD function retrieves values from a constant offset within the SMF record. It has the following syntax: SMF_FIELD(*offset in record,length*). Both the offset and the length are in decimal; offset 0 indicates the start of the record (the length field). When used, the SMF_FIELD reads a value from the SMF record at the indicated offset, with the indicated length (it will not read beyond the end of the SMF record, but truncate the field instead). Offsets and lengths of SMF fields are documented in the "MVS System Management Facilities (SMF)" manual.

For example, the DATE field in an SMF record resides at offset 10 and has length 4. You can define this field yourself using the following construction:

```
define type=SMF mydate(date) as smf_field(10,4)
newlist type=SMF
select mydate=01jan1996
sortlist mydate
```

The following example shows how to make a dump of SMF records.

```
newlist type=smf t='hex dump of smf records'
define smf_record as smf_field(0,32767)
sortlist recno smf_record(dump)
```

SMF_SECTION

The SMF_SECTION function specifies retrieves values described by a so-called self-defining section within the SMF record. This is a triple of (offset,length,number) values describing a repeated section in an SMF record, e.g. the product section in SMF 30. The SMF_SECTION function has the following syntax: SMF_SECTION(*offset to triple*) or SMF_SECTION(*offsettotriple, offset within section,length*). All values are in decimal; offset 0 indicates the start of the record (the length field) or the start of the triple. The version with one parameter uses the whole of the repeated section; the other version uses a specific part of the section. When used, the SMF_SECTION reads one value from the SMF record for each such triple in the record (it will not read beyond the end of the SMF record). Offsets and lengths of SMF fields are documented in the "MVS System Management Facilities (SMF)" manual.

For example, the subsystem section field in an SMF 30 record is described by a triple at offset 24. The subsystem or product id resides at offset 6 and has length 8.

```
define type=SMF id(char) as smf_section(24,6,8)
newlist type=SMF
select id=smf
sortlist date time jobname id
```

All three types of construct can then be used in SELECT/EXCLUDE processing, and in output processing. The overriding format specified (CHAR, DEC, or DATE in the preceding examples) determine both the input format and the output format. If the field is only valid under certain circumstances, these can be specified using a

WHERE clause in the DEFINE. The field is only available if the WHERE clause is true; otherwise it is missing. For instance, the specification of SMF 30 can be added to the definition. The following example shows how the field can be defined and used:

```
define id(char) as smf_section(24,6,8) where type=30
newlist type=SMF
select id=smf
sortlist date time jobname id
```

Tutorial: Reporting on a user log

In the following section we will show you how the define statements needed to analyze the HTTP error log were built. You can use this as a guideline when creating the CARLa for reporting on any log files needed. We will start with the simplest case, and add complications and their solutions as we go.

First we issue a DEFTYPE command to give our new NEWLIST type a unique name.

```
deftype type=$HTTPERROR
```

The $ character has been included to ensure that there is no predefined type with the same name. Any national character (@, $ or #) can be used for that purpose.

Next we take a look at a single record in the HTTP error log. The simplest looks as follows:

```
[04/May/2001:08:22:54 -0100] IMW0487E Persist timer expired while
   waiting on client 10.0.96.4
```

A date, time and time zone specification between square brackets, followed by the error message issued.

A first shot at parsing this could be

```
define type=$HTTPERROR datetime as parse(record,'[',']')
define type=$HTTPERROR error as parse(record,']')
```

This creates two fields. DATETIME will contain the text present between the square brackets, and ERROR will contain everything after the closing bracket up to End-Of-Line. Both fields can be used directly, but they can still be improved. The ERROR field as we have defined it now still starts with a blank, and the DATETIME field will be treated as if it was a normal string of text. It will sort incorrectly, and select functions built specifically for dates and times will not work for it.

Improving the ERROR field is simple. Just include the blank in the starting delimiter.

```
define type=$HTTPERROR error as parse(record,'] ')
```

For the DATETIME field we need to add a convert function to change the text field to a date/time field.

```
define type=$HTTPERROR datetime as convert(parse(record,'[',']'),datetime)
```

Now functions like select will treat this field as a time stamp, thus allowing you to select on it and sort it at will.

However, we have lost some information: the time zone is not remembered in datetime convert processing. If we still want to report it, we need to create a new

field for it. The time zone is everything after the blank in the string between the square brackets. We could find this with another parse command, but this time we will use word to do it.

```
define type=$HTTPERROR timezone as word(parse(record,'[',']'),2,' ')
```

The parse still gives us the text between the brackets, but now we use the word function to split it in two parts: everything before the blank, and everything after it. Our field will be the second part.

There are several other possibilities for the convert function as well. If you want to report on the day of the week the record was written, you could use define

```
type=$HTTPERROR weekday as convert(parse(record,'[',']'),datetime,weekday)
```

There are also records in the log that look different:

```
[04/May/2001:08:16:48 -0100] [IMW0210E MULTI FAILED] [host: 10.0.96.4
     user:c####r1] /c####/AutoHelpdesk.html
[04/May/2001:08:26:34 -0100] [IMW0196I NOT AUTHENTICATED]
     [host: 10.0.96.4] /c####/Helpdesk.htm
[04/May/2001:11:25:20 -0100] [IMW0193I OK] [host: 10.0.96.2
     user: c####r1 referer: https://10.0.1.22/c####/Helpdesk.html] IMW0532E
 ReadContent..Premature End Of File on socket 23 - reason 1
```

There are several differences here: a message in a second set of brackets, some identification in a third set and either a file or a second message as final part of the record.

To get the error that is shown in the second set of brackets we can use a parse with a start delimiter of ' [' (blank bracket), to differentiate the opening bracket of the second set from that of the first. We can also separate the record into different parts with word and the open bracket as delimiter. We will use the latter method, because it is easier to extend for the third set of brackets. There are two issues with this method. One is that we need to keep in mind that the first open bracket, even though nothing precedes it, separates the first "word" of the record from the second, so that for the text after the second bracket we need the third "word". The other is that we still need to trim the closing bracket and its trailing space from our text. We do this with another word function, this time with the close bracket as delimiter.

```
define type=$HTTPERROR error2 as
   word(word(record,3,'['),1,']')
define type=$HTTPERROR identifier as
   word(word(record,4,'['),1,']')
```

Now we want to split the identifier in host, user and referrer fields. We do this with a parse, looking for the host: text. If we include the blank in our starting delimiter, we can use the blank preceding the next identifier as our ending delimiter.

```
define type=$HTTPERROR host as
   parse(word(word(record,4,'['),1,']'),'host: ',' ')
define type=$HTTPERROR user
   as parse(word(word(record,4,'['),1,']'),'user: ',' ')
define type=$HTTPERROR referer
   as parse(word(word(record,4,'['),1,']'),'referer: ',' ')
```

The tail of the record can be picked up with another word call, taking everything after the third closing bracket. To remove the leading blank from the field we need

to use the substring function. We cannot simply add the blank to the delimiter like we did for the parse earlier because word only accepts a single character as delimiter.

```
define type=$HTTPERROR tail as substring(word(record,4,']'),2)
```

The substring specification here is: from the second character until End-Of-Line.

Actually, we don't want to call this field tail. In some cases it is an error message, and in some cases it is a file. So how do we differentiate between the two? Since file names can contain all characters that the error message can contain, this is easier said than done. In our log, all files are shown with absolute pathnames, so start with /, and all messages start with IMW. We could use either of these criteria, but we need to keep in mind that these are not guaranteed to be true. For now we'll use the slash to positively identify a file and keep an eye out for anomalies.

```
define type=$HTTPERROR firstchar as
   substring(word(record,4,']'),2,1)
```

We define a field FIRSTCHAR that contains only the one character we will use for the differentiation. We do that by specifying a length of one on the substring. This field can then be used in a where clause.

```
define type=$HTTPERROR file as
   substring(word(record,4,']'),2) where firstchar='/'
define type=$HTTPERROR error3 as
   substring(word(record,4,']'),2) where firstchar<>'/'
```

By now we have defined three error fields while we usually only want to show one message, so we need some more where clauses to make sure only one is actually filled in. Our original ERROR field is only valid when ERROR2 is not present, and we probably do not want to show the OK message in ERROR2 when there is an ERROR3 present. This means we only want ERROR2 when there is no ERROR3, and ERROR only when we have neither.

```
define type=$HTTPERROR error3 as
   substring(word(record,4,']'),2) where firstchar<>'/'
define type=$HTTPERROR error2 as
   word(word(record,3,'['),1,']')where missing(error3)
define type=$HTTPERROR error as
   parse(record,'] ')where missing(error3) and missing(error2)
```

These three fields can then be shown concatenated:

```
   sortlist error3(0) | error2(0) | error(0)
```

The defines as presented here are missing some output modifiers. Ideally, they should have a default format, output length and column header specification. All defines inherit these from the RECORD field except the DATETIME field. The DATETIME field gets the *datetime* format from the convert function and the WEEKDAY, which gets the weekday format. The format inherited from the RECORD field is ASIS, which has specifically been built to keep trailing spaces intact. If you want those trailing spaces trimmed in your output, you should use output format CHAR as shown in this code sample:

```
define type=$HTTPERROR file('Target file' char 30) as
   substring(word(record,4,']'),2) where isfile='/'
```

Another caveat, specific to this example: EBCDIC includes two different sets of square brackets: 1) `x'BA'` and `x'BB'` , and 2) `x'AD' and x'BD'`. When using square brackets in these field value manipulation functions, verify that you are using the set that is actually present in your logfile.

Title, format and output length

The newly defined field will inherit the default values (they can be overridden, see "Parameter syntax: Specifying parameters for LIST/SORTLIST/DISPLAY commands" on page 796) these characteristics from the base field. There are the following exceptions to this:

- Indirect references These fields will have the default output format of the target of the reference.
- Converted fields These fields will have the default output format corresponding with the selected internal format.

Example: Basic summary statistics

The basic use of the DEFINE command for summary statistics is illustrated in the following example:

```
define cnt count                 /* Count selected instances */
define permits sum(aclcnt)       /* Sum of the number of ACL entries */
define maxacl max(aclcnt)        /* Highest number of ACL entries */
define maxacs max(useracs)       /* Highest access of ACL entries */
define frq freq                  /* Relative frequency */
summary class cnt frq permits maxacl maxacs
```

This shows, for each class of profiles, the number of profiles, the total number of entries on all of the access lists in that class, the largest access list, and the highest level of access.

Example: count and sumcount

The following example shows the use of COUNT and SUMCOUNT. As is shown, COUNT indicates the number of instances summarized, and SUMCOUNT indicates the number of distinct cases found.

```
/* Show difference between count and sumcount */
newlist type=racf
 select class=user segment=base mask=utst*
 sortlist class key(8)
 define diff_keys sumcount
 define records  count
 summary class diff_keys * key(6) records
```

```
Class    DIFF_KEY Profil RECORDS  Class    Profile
USER            3              13
                  UTST2$        4
                                   USER     UTST2$S
                                   USER     UTST2$T
                                   USER     UTST2$U
                                   USER     UTST2$V
                  UTST2#        5
                                   USER     UTST2#R
                                   USER     UTST2#S
                                   USER     UTST2#T
                                   USER     UTST2#U
                                   USER     UTST2#V
                  UTST2@        4
                                   USER     UTST2@S
                                   USER     UTST2@T
                                   USER     UTST2@U
                                   USER     UTST2@V
```

Of the thirteen users selected, there are three different cases when using the first 6 characters only.

Example: WHERE clause for summary statistics

The use of a conditional clause is illustrated in the following examples:

```
/* Count selected instances that also have userid=ibmuser */
define cnt count where userid=ibmuser

/* Count frequency of selected instances that also have UACC>=READ */
define uacchigh freq where uacc>=read
summary class cnt uacchigh
```

The variable *cnt* counts the amount of summarized records that have user ID=IBMUSER. Similarly, the variable UACCHIGH describes the relative frequency of occurrences with UACC>=READ among the summarized occurrences.

Example: Boolean variable with SORTLIST

The use of a WHERE clause to define a Boolean variable that can be used with a SORTLIST command is shown in the following example:

```
/* Set variable to TRUE if profile was created in last month */
define recent boolean where creadate>today-31
sortlist profile recent
```

Example: Sharing a WHERE clause

The use of the COUNT, FREQ, and BOOLEAN types with a shared WHERE clause is illustrated in the following examples:

```
/* Variable with WHERE clause that is to be shared */
define recent boolean where createdate>today-31

/* Relative frequency of recent instances */
define recfreq freq(recent)

/* Count the number of selected recent instances */
define reccnt count(recent)
```

In the example, the RECFREQ and RECCNT variables use the WHERE clause defined with the Boolean variable RECENT.

Example: subselect access list

A subselected variable displays only those ACL instances that match the subselect clause. The ACL modifiers EXPLODE (display all possible access), RESOLVE (for each user who has access via the ACL, list the highest access) and EFFECTIVE(as RESOLVE but also include access by other means than via the ACL) can be used, both in the variable definition and on the DISPLAY/SORTLIST (the latter overrides the former). In the following example, only those ACL entries are selected that have an access of UPDATE or higher, or that are conditional access list entries of type PROGRAM. The original access list is shown in the preceding section.

```
newlist
 select class=dataset key=sysappl.cnracf.**
 define demoacl subselect acl(access>=update or whenclass=program)
 display key(20) demoacl

Profile key          User     Access  ACL id   When
SYSAPPL.CNRACF.**    R##PSEC  UPDATE  R##PSEC
                     R##PROB  ALTER   R##PROB
                     R##BDAG  UPDATE  R##BDAG  PROGRAM  CNRACF
                     C##AINT  READ    C##AINT  PROGRAM  CNRACF
                     R##PTST  READ    R##PTST  PROGRAM  CNRACF
```

Example: subselect user in access list

In the following example, all data set profiles are selected that have user IBMUSER in their access list. Of those profiles, the exploded access list is subselected for user IBMUSER; this displays all types of access the user has on the profile. RESOLVE would have displayed the highest access of IBMUSER; if no output modifier had been used, only the access list entries for IBMUSER would have been displayed.

```
newlist
 select class=dataset userid=ibmuser
 define ibmacl(explode,sort) subselect acl(user=ibmuser)
 display key(20) ibmacl
```

```
Profile key          User     Access  ACL id   When
C##HANS.TEST.BIG.PRO IBMUSER  NONE    IBMUSER
IPCS.*.**            IBMUSER  ALTER   IBMUSER
                     IBMUSER  ALTER   SYS1
SYS1.*.**            IBMUSER  ALTER   IBMUSER
                     IBMUSER  ALTER   SYS1
SYS1.BRODCAST        IBMUSER  ALTER   IBMUSER
SYS1.CMDLIB          IBMUSER  ALTER   IBMUSER
SYS1.CMDPROC         IBMUSER  ALTER   IBMUSER
SYS1.COBLIB          IBMUSER  ALTER   IBMUSER
SYS1.DIRACC          IBMUSER  ALTER   IBMUSER
SYS1.DIVERSEN.*.**   IBMUSER  ALTER   IBMUSER
SYS1.DUMP*.**        IBMUSER  ALTER   IBMUSER
SYS1.LOGREC          IBMUSER  ALTER   IBMUSER
SYS1.MAN*.**         IBMUSER  ALTER   IBMUSER
SYS1.PLI*.**         IBMUSER  ALTER   IBMUSER
SYS1.PRODUCTS.*.**   IBMUSER  ALTER   IBMUSER
SYS1.RC.HELP         IBMUSER  ALTER   IBMUSER
SYS1.UADS            IBMUSER  ALTER   IBMUSER
```

Notes: The selection only selects profiles that have IBMUSER on the access list. Profiles where IBMUSER does not have direct access, e.g. because he only has indirect access through a group id on the access list, are not included. To select all profiles and all reasons that a user has access, use the NEWLIST SCOPE parameter, e.g. SCOPE=IBMUSER, or use the REPORT SCOPE.

Example: subselect connect instances

In the following example, all user profiles are selected that have one or more group-SPECIAL attributes. Of the group-connects, only those that are group-special are printed.

```
newlist
 select class=user grpspec
 define specs subselect connects(grpspec)
 display key(8) specs
```

```
Profile  User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt
UCNGADM  GCNGTG   USE       S A    NONE
UCNG002  GCNGT    USE       S      NONE
UTST2#R  GROUP1   USE     R S A AG NONE
```

The next example selects all user profiles that have 2 or more group-connections. One of these is always the default-group. The query displays only the non-default group connections. Note the use of a field-to-field comparison instead of a field-to-constant comparison.

```
newlist
 select class=user congrpct>1
 define nondflt(8) subselect connects(group<<>>user:dfltgrp)
 display key(8) dfltgrp nondflt
```

```
Profile  DfltGrp  User/Grp
IBMUSER  SYS1     OMVGRP
                  SYSCTLG
                  VSAMDSET
UCNGADS  GCNGTG   SYS1
UTST2$T  GROUP1   VSAMDSET
UTST2$U  GROUP1   VSAMDSET
UTST2$V  GROUP1   VSAMDSET
UTST2#T  GROUP2   VSAMDSET
UTST2#U  GROUP2   VSAMDSET
UTST2#V  GROUP2   VSAMDSET
```

Example: subselect custom field

The following example shows data all users in the department that is stored in the custom field DEPT.

```
newlist type=racf
define department(8) subselect custom_data(cskey=dept)
select class=user segment=csdata
sortlist key(8) department
```

Notice however that this simple example could have been coded more easily as:

```
newlist type=racf
select class=user segment=csdata exists(dept)
sortlist key(8) dept
```

Example: summary statistics with WHERE clause

The following example shows the use of WHERE clauses for variables used with a SUMMARY command. Summary variables with a WHERE clause are updated only if the WHERE clause is true, whereas variables without a WHERE clause are updated for each occurrence summarized.

```
newlist type=racf
 define class#('#profiles' 9) count
 define class@('%profiles' 9) freq
 define generic#('#gen in class' 13) count where generic
 define generic@('%gen in class' 13) freq where generic
 summary class class# class@ generic# generic@
```

Class	#profiles	%profiles	#gen in class	%gen in class
ACCTNUM	3	0	1	33
AIMS	2	0	0	0
APPCLU	47	1	1	2
APPCPORT	12	0	0	0
APPCSERV	2	0	1	50
APPCTP	2	0	1	50
APPL	18	0	0	0
CCICSCMD	2	0	0	0
CONSOLE	4	0	1	25
CSFKEYS	1	0	1	100
CSFSERV	1	0	1	100
DASDVOL	3	0	1	33
DATASET	1111	29	1084	97
DCEUUIDS	1	0	0	0
DIGTCERT	48	1	0	0
DIGTCRIT	2	0	0	0
DIGTNMAP	4	0	0	0
DLFCLASS	5	0	3	60
DSNR	1	0	0	0
FACILITY	382	10	134	35
FIELD	89	2	15	16
GCICSTRN	3	0	0	0
GLOBAL	3	0	0	0
GROUP	285	7	0	0
GSDSF	1	0	0	0
IBMOPC	2	0	1	50
JESINPUT	2	0	0	0
JESJOBS	1	0	1	100
JESSPOOL	41	1	41	100
NETCMDS	2	0	1	50
NETSPAN	1	0	1	100
NODES	12	0	11	91
OPERCMDS	39	1	29	74
PERFGRP	1	0	1	100
PROGRAM	45	1	0	0
PTKTDATA	24	0	1	4
RACFVARS	8	0	0	0
ROLE	10	0	0	0
RRSFDATA	9	0	4	44
SDSF	33	0	18	54
SECDATA	2	0	0	0
SECLABEL	6	0	0	0
STARTED	266	7	264	99
SURROGAT	41	1	5	12
SYSMVIEW	8	0	2	25
TAPEVOL	20	0	14	70
TERMINAL	4	0	1	25
TSOAUTH	7	0	0	0
TSOPROC	19	0	3	15
UNIXMAP	92	2	0	0
USER	1030	27	0	0
VMCMD	1	0	0	0
VMMDISK	5	0	4	80
VMPOSIX	12	0	1	8
VTAMAPPL	11	0	0	0
WRITER	1	0	1	100

Example: Defining a <deftype> file

```
deftype type=email
define type=email user as word(record,1,' ')
define type=email address as word(record,2,'40'X)
```

DEFTYPE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The DEFTYPE command can be used to define a NEWLIST type which can then be used on the following commands:

1. ALLOCATE to allocate the files which are to be read for the new type
2. DEFINE to specify the fields that can be used in reporting on this data
3. NEWLIST to report on the contents of the new type of data
4. indirect references to this data

The parameters recognized by the DEFTYPE command are the following:

ABBREV2= *abbreviation*
This optional parameter sets the two character abbreviation used to create default ddnames for the files that will be allocated. The DDnames are of the format CKR@*aaxx* where *aa* is the abbreviation specified and *xx* is a counter from 0 to 99 too keep multiple files for the same <deftype> separate.

When running under ISPF, the @ is replaced by a logical screen indicator (1, 2, ..9, A, B, ...). It is advisable to include a national character in this parameter, to avoid conflicts with predefined NEWLIST types.

DETAILHELPPANEL= *panel*
This indicates which help panel to use when there is no field level help panel available or requested and there is no DETAILHELPPANEL specified on the NEWLIST or OPTION statement, and HELP is pressed on the detail display of a DISPLAY or DSUMMARY. The panel name specified may contain "&CKREREL." to be replaced with 2 or 3 depending on the ISPF level (2 for VM), but not in the first position. If this parameter is omitted, C2R&CKREREL.NN#0 is used. The parameter must be specified before the field name, similar to the TYPE= specification.

HELPPANEL= *panel*
This indicates which help panel to use when there is no field level help panel available or requested and there is no help panel on the NEWLIST or OPTION statement appropriate for the current display level (HELPPANEL, or SUMHELPPANEL), and HELP is pressed on the summary or overview display of a DISPLAY or DSUMMARY. The panel name specified may contain "&CKREREL." to be replaced with 2 or 3 depending on the ISPF level (2 for VM), but not in the first position. If this parameter is omitted, C2R&CKREREL.NN@0 is used. The parameter must be specified before the field name, similar to the TYPE= specification.

NOWARN
This parameter can be used to turn off the check for national characters in the TYPE and ABBREV2 specifications. When this parameter is not specified, message CKR1308 is issued when no national character is used in either the TYPE or ABBREV2 specification. This message provides a warning about possible conflicts with predefined NEWLIST types that might occur.

TYPE= <*deftype*>
This sets the name of the DEFTYPE, to be used in the ALLOCATE/DEFINE and NEWLIST commands. It can be up to 24 characters long and can contain

characters, digits and the national characters. It is advisable to include a national character in this parameter, to avoid conflicts with predefined NEWLIST types.

DISPLAY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

You can use the DISPLAY command for showing the contents of arbitrary selected data interactively in an ISPF panel. When you create standard reports from the product menus, the DISPLAY command is automatically generated when needed. You only need to specify the command if you want to create customized ISPF panels. You can also specify the command using the abbreviation D. The command syntax is identical to the syntax for the LIST and SORTLIST commands, which is described in "LIST family of commands" on page 794. The sort order is the same order specified in the "SORTLIST" on page 918 command.

If the DISPLAYTOFILE format is specified, the DISPLAY command acts like a SORTLIST command if the PRINT or NEWLIST option is also set. This print specification turns an ISPF report into a batch report.

When a field in a DISPLAY statement is specified with the WORDWRAP or WRAP modifier, the field is shown in the Detail ISPF display panel but not in the Overview display panel.

DSUMMARY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

The DSUMMARY command is almost equal to the SUMMARY command, which is described in "SUMMARY" on page 918. The difference between the two is their behavior as influenced by the environment (ISPF or batch) and the combination with detailed information (when combined with DISPLAY or SORTLIST). The following table shows the difference in behavior.

	SORTLIST	DISPLAY	No detail
DSUMMARY	ISPF	ISPF	ISPF
SUMMARY	file	ISPF	file

The DSUMMARY command always generates an interactive ISPF summary, while the SUMMARY command only does so when combined with DISPLAY.

ENDBUNDLE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command terminates a BUNDLE. The print options present before the BUNDLE command are restored.

ENDMERGE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command terminates a MERGELIST. The options and scope determined by the last NEWLIST encountered (either in or before the MERGELIST) remain in effect. A subsequent NEWLIST is *not* merged.

This command is also used to end a MERGE command, see "MERGE" on page 836.

FILEOPTION

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The `FILEOPTION` statement sets file options for the specified ddname. If you want to specify global file options, use the `OPTION` command. See "OPTION" on page 856.

The first `FILEOPTION` statement for a particular ddname also applies file options specified on previous `OPTION` statements insofar as these statements are not overridden by the FILEOPTION statement itself. Multiple FILEOPTION statements can be given for the same ddname, but they must precede the first NEWLIST that refers to that ddname. A NEWLIST can refer to a ddname explicitly by the DD= parameter, or implicitly by the DD= parameter of a previous OPTION command.

File options can also be specified on an individual NEWLIST. However, some file options must be the same for all NEWLISTs written to a particular ddname. You cannot override these options (FILEFORMAT=XMLand ENCODING=UTF-8 for example). Others can only be partially honored if they differ across newlists (e.g. NOPAGE and PAGELEN=nn influence whether a new data set gets allocated with RECFM=A or not).

Note that FILEOPTION can also be used for emailed newlists. If the emails are really emailed (not using option SMTPTOFILE) you should use DD=C2REMAIL on the FILEOPTION statement. If SMTPTOFILE is used, you should use DD=C2RSMTP.

As an example, the following commands write a "mount" report to DD MYREPOR1, which uses a page length of 64. The sensitivity report is written to the DD MYREPOR2 which uses a page length of 32.

```
fileoption dd=myrepor1 pagelength=64
fileoption dd=myrepor2 pagelength=32

option dd=myrepor1

newlist type=mount
 sortlist system mountpoint dsname volser

newlist type=sensitive dd=myrepor2
 sortlist auditpriority sensitivity dsname volser risk auditconcern
```

Note that for a MERGELIST the FILEOPTION parameters are taken from the first NEWLIST statement within the MERGELIST/ENDMERGE statement. The parameters from the other NEWLISTs are ignored.

The following parameters can be specified as FILEOPTION. The list describes what happens with NEWLISTs that *effectively* have this parameter (whether it is specified on a FILEOPTION command or directly on the NEWLIST).

CAPS
Output is only in uppercase.

Limitation: DBCS characters in the output for a `NEWLIST` statement are not affected by the `CAPS` option if the corresponding `NEWLIST` statement also has a DBCS option. In all other cases, including a listing of the input commands, DBCS characters are not preserved.

COMPRESS=[GZIP]
This parameter can be used to request that the output file is created in gzip format according to RFC 1952. This only works for UNIX files that have been allocated with an ALLOC command with a FILEDESC or PATH specification, see "ALLOCATE" on page 718. The default compression level of 6 is used. This parameter is invalid in combination with CMD, WTO, SNMP, and MAIL. It cannot be used with a DISPLAY command.

DD= *ddname*
ddname=*ddname*
FILE=*ddname* **F=***ddname*
This defines to which output file the FILEOPTION statement applies. This parameter is required.

ENCODING=EBCDIC
ENCODING=UTF-8
Output will be in the specified character encoding. By default the character encoding is EBCDIC. The advantage of UTF-8 output files is that values that are natively in Unicode format (e.g. Unicode DB2 fields) can in fact be processed preserving their value. The default, EBCDIC, means that any values in UTF-8 get converted to the best EBCDIC representation possible, exploiting substitute characters where no proper mapping exists.

Note that an UTF-8 file can be a Unix file or a data set. UTF-8 data sets cannot be processed well on the mainframe except to copy or FTP to another file format. Specifically, the ASA carriage control column in RECFM=VBA data sets will contain page or line feeds in UTF-8, and RECFM=VB files are not generated with a line feed per record at all.

The option ENCODING=UTF-8 is mutually exclusive with WTO, SNMP, and CMD.

If the proper `UNICODE` environment has not been set up, the `CKR0917` message is issued, and the run terminated. By suppressing this message, fallback to a simple low-128 ASCII translation scheme is possible, but this is not the best option for production purposes.

Example:

To sent out a UTF-8 encoded report in an email attachment, you can use the following CARLa.

```
fileoption dd=C2REMAIL encoding=UTF-8

newlist type=racf,
  mailto=rcpt@exampledomain.com,
```

```
 from=sender@exampledomain.com,
 outputformat=attach
select class=user segment=base special
sortlist key(8) pgmrname
```

FILEFORMAT=XML
FILEFORMAT=TEXT

This keyword can be used to specify the format of an output file. TEXT specifies that no special formatting will be done.

XML means that the output file should be in the form of an XML (Extended Markup Language) document. The specification of FILEFORMAT=XML is mutually exclusive with NEWLIST options WTO, CMD, SNMP, and PAGELENGTH, and with the DISPLAY command.

For any field written to be written to an FILEFORMAT=XML file, output modifiers TOPTITLE, TITLE, PAGE, PREFIX, and WRAP are forbidden. Literal strings currently have no meaning and are forbidden. However, a fixed literal content for an element can be created by a DEFINE element(HB ,"literal") TRUE.

The XML document generated will follow the general structure for XML: a header, a DTD (Document Type Definition) describing the document structure, and a single root element that contains the actual information output by LIST/SORTLIST/SUMMARY. The single root element is the ddname (filename) chosen. The root element has the `creation=` attribute for the creation time stamp in `xsd:dateTime` format. The structure of the rest of the document with the actual NEWLIST-specific output depends on whether there is a MERGELIST specification or not.

Without a MERGELIST, one data element per NEWLIST record will be written. The element name for a NEWLIST record is taken from the NEWLIST NAME= parameter. Hence this parameter is required with FILEFORMAT=XML. Within the NEWLIST record element, a sub-element will be present per non-empty field specified on the (SORT)LIST/SUMMARY statement. If the field is missing, then the sub-element will be omitted. When a field has multiple values, the sub-element will be repeated (unless the HORIZONTAL modifier is used). A field name can only occur once per NEWLIST. A field name cannot be the same as a NEWLIST name that is being output to the same XML document (output file).

Example:

```
fileoption dd=myxml fileformat=xml
n dd=myxml type=system name=SYS
 list system mvslvl
```

Creates XML document body:

```
<MYXML creation="2005-12-06T14:12:32.66+01:00">
<SYS>
<SYSTEM>DINO</SYSTEM>
<MVSLVL>SP7.0.4</MVSLVL>
</SYS>
</MYXML>
```

If there is a MERGELIST specification, the records within the mergelist are output as an element with a common name set to the MERGELIST NAME= parameter. The fields that are shared between all mergelist members are output as sub-elements of the NEWLIST type element. The non-shared fields are encapsulated in an element set to the member NEWLIST NAME= parameter (as for the non-MERGELIST, case but as a sub-element of the MERGELIST).

Example:

```
fileoption dd=myxml fileformat=xml
mergelist name=SOFTWARE dd=myxml
n type=system name=MVS
 list system mvslvl
n type=system name=ESM
 list system esmlvl
endmerge
```

Creates XML document body:

```
<MYXML creation="2005-12-07T15:23:04.78+01:00">
<SOFTWARE>
<SYSTEM>DINO</SYSTEM>
<MVS>
<MVSLVL>SP7.0.4</MVSLVL>
</MVS>
</SOFTWARE>
<SOFTWARE>
<SYSTEM>DINO</SYSTEM>
<ESM>
<ESMLVL>HRF7707 OA03853</ESMLVL>
</ESM>
</SOFTWARE>
</MYXML>
```

LINELEN= *value*
LINELENGTH=*value* **LL=***value*
This option can be used to set the length of lines that are output by Security zSecure. If Security zSecure controls the LRECL specification of the output DD (when calling from JCL with no LRECL= specification, or when dynamically allocating the data set), this parameter influences the LRECL of the resulting data set. Security zSecure uses the largest line length found for all NEWLISTs directed to a particular file. If Security zSecure writes to an existing data set, or LRECL= is specified for the file, the line length cannot become larger than this value.

To get the page number in the proper position for a narrow print, specify LL=79.

MAXP= *number*
MAXPAGE=*number*
PRTMAXP=*number*
This parameter can be used to limit the amount of output that is actually printed. All data is still read and formatted, but printing will stop the moment the specified number of pages has been reached.

NONULLS
This keyword can be specified to turn off the printing of hexadecimal nulls in the (sort)list report(s). They will be replaced with blanks. See also the NULLS keyword. Note that with XML output, trailing null characters are trimmed off; other null characters are replaced by · (a bullet character).

NOPAGE
This option suppresses all titles and headers which would normally be written above each page for sortlist output. If Security zSecure controls the RECFM specification of the output DD (when calling from JCL with no RECFM= specification, or when dynamically allocating the data set), and all NEWLISTs writing to this DD effectively have NOPAGE, then Security zSecure creates a RECFM=VB data set; otherwise a RECFM=VBA data set.

NOXML_DATADICT
This option turns off generating a data dictionary when XML output is requested (option FILEFORMAT=XML). See also option XML_DATADICT. By default the data dictionary is not generated.

NOXML_DTD
This option turns off generating a DTD (Document Type Definitions) when XML output is requested (option FILEFORMAT=XML). See also option XML_DTD. By default the DTD will be generated unless XML_STYLESHEET=IMBED has been specified.

NULLS
This keyword can be specified to turn on the printing of hexadecimal nulls in the (sort)list report(s). This is the default setting. See also the NONULLS keyword. Note that with XML output, trailing null characters are trimmed off; other null characters are replaced by · (a bullet character).

OVERPRINT= *number*
OVP=*number*
Number of overprints to get bold text on impact printers. Values must be in the range 0 to 9. Specifying 0 disables overprinting, and is the default. It is only used if the output file has RECFM=A and OPTCD=J is *not* included in the DCB parameters of the DD.

PAGELEN=number
PAGELENGTH=number PL=number
Number of lines on each page to be used for printing. The default is 0 for LIST commands in the domain of a NEWLIST, and 56 for SORTLIST commands, and for the files SYSPRINT and CKREPORT. The minimum is 6, the maximum is 32767.

PL=0 is equivalent to specifying NOPAGE, except that PL=0 prints page headers on the first page in the output file. You should use NOPAGE with (SORT)LIST to suppress page headers, e.g. for command generation.

If Security zSecure controls the RECFM specification of the output DD (when calling from JCL with no RECFM= specification, or when dynamically allocating the data set), and all NEWLISTs writing to this DD *effectively* have PL=0, then Security zSecure creates a RECFM=VB data set; otherwise a RECFM=VBA data set.

The PL= option is ignored with FILEFORMAT=XML; NOPAGE is implied instead.

SMTPCLASS= *sysoutclass*
Specifies the JES output class to be used for the SMTP output processing of emails. When no class is specified, email will be sent to the default class, B.

SMTPNJENODE= *nodename*
Specifies the JES destination to which emails will be routed for final processing. If the SMTP server is running on your local system, this keyword can be omitted.

SMTPWRITER= *name*
Specifies a name for use in SMTP selecting an email SYSOUT data set. The external writer name is equal to the SMTP address space name. When no writer is specified, email will be sent to the default writer, "SMTP".

TOPTITLE= *text*, **TT SUBTITLE=***text*, **ST TITLE=***text*, **T PAGETEXT=***text*
Titles to appear on subsequent output pages. TOPTITLE redefines the page header.

TOPTITLE is only used for LIST/SORTLIST/DISPLAY outside ISPF. TITLE redefines the title line printed below the top title line; SUBTITLE defines a line to be printed below the title line. TITLE and SUBTITLE are also used by DISPLAY commands inside ISPF and by REPORT and VERIFY output. The TOPTITLE parameter redefines the page header string only; the page indicator, page number and date are still printed. The PAGETEXT parameter can be used to redefine the page indicator, which is 'page' by default. The syntax requirements for the title are:

title='*string*'
title="*string*"
title=`*string* `
title=:*var*

The title string can be specified as a string enclosed in single, double or left quotation marks. The string can cross the line boundary, simply continue typing at the start of the next line. In the command listing, the string continuation is indicated by a + following the line number. Alternatively, an ISPF variable name can be passed prefixed by a colon. The content of the ISPF variable is used as the title. The implicit function pool, shared variable, and profile pool will be searched for the variable name.

See also “General output modifiers: Controlling field-related output” on page 798: title and toptitle.

XML_DATADICT
This option turns on generating a data dictionary when XML output is requested (option FILEFORMAT=XML). The data dictionary contains information about the characteristics of each generated report: the title, top title, and subtitle, and at the field level the field's format, its effective width, its alignment, its (prefix) header, and an indication whether it is a repeated field.

These formatting hints can be exploited by XSLT stylesheets so that many reports can be accommodated by a single stylesheet. Using a data dictionary is required when using the XSLT stylesheet supplied with IBM Security zSecure. See also option XML_STYLESHEET.

This option can be overridden with NOXML_DATADICT. By default the data dictionary is not generated.

XML_DTD
This option turns on generating a DTD (Document Type Definitions) specification when XML output is requested (option FILEFORMAT=XML). This specification can be used by XML processors to validate the document, and to get a better understanding of the structure of the XML document.

This option can be used to override an earlier NOXML_DTD. It cannot be specified when requesting an imbedded stylesheet using XML_STYLESHEET=IMBED. By default the DTD will be generated unless XML_STYLESHEET=IMBED has been specified. See also option NOXML_DTD.

XML_STYLESHEET=NO
XML_STYLESHEET=URI("*uri***")**
XML_STYLESHEET=IMBED(ddname=*ddname***,MEMBER=***member***)**
When `XML_STYLESHEET=URI("uri")` is specified, an `<?xml-stylesheet type="text/xsl" href="uri"?>` processing instruction is added to the prolog of the XML document. Make sure that the recipient of the report has access to the XSLT stylesheet identified by the URI specified in the processing instruction.

When XML_STYLESHEET=IMBED(ddname=*ddname*,MEMBER=*member*) is specified, the XML data is imbedded in the specified XSLT stylesheet, resulting in one output file containing both the XSLT stylesheet and the XML data. A processing instruction is added to transform the XML document by itself, so opening just this one XML file with a web browser (or any other program that supports XSLT stylesheets) shows the transformed result. You can use imbedding to guarantee that the recipient of the report has the XSLT stylesheet available. You can omit the ddname= clause; by default the CARLa library is used. The resulting XML data must be saved with extension xml, or served as mimetype application/xml. You can find an example of an XSLT stylesheet to transform the XML data to nicely formatted HTML tables in member C2RXSL01 in the SCKRCARL data set. The stylesheet is also available on the web: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.13/c2rxsl01.xsl. This generic XSLT stylesheet can transform most tabular reports specified in CARLa. Using this XSLT stylesheet allows looking at the data in a web browser, and importing the data into Microsoft Excel 2002 and up.

The stylesheet supplied with IBM Security zSecure can be used for both linking from the XML, and imbedding the XML, for example, with

```
fileoption dd=output fileformat=xml xml_datadict
   xml_stylesheet=uri("http://publib.boulder.ibm.com/infocenter/
                       tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.12/c2rxsl01.xsl")
```

or

```
fileoption dd=output fileformat=xml xml_datadict xml_stylesheet=imbed(m=c2rxsl01)
```

Note that for security reasons, most web browsers do not transform an XML document on one internet domain with an XSLT stylesheet from another domain. You may need to copy the XSLT stylesheet to your own domain, or copy it to the local disk, or use imbedding.

To use the stylesheet supplied with IBM Security zSecure, an XML data dictionary must be included with the XML. See "XML_DATADICT" on page 784. The XSLT stylesheet only handles tabular reports. If a MERGELIST report is created, all columns in all SORTLIST/SUMMARY statements in the MERGELIST must be the same. The title used on the generated HTML page is the default top title or explicit TOPTITLE from the first NEWLIST in the report. Every separate report shows the title and subtitle specified on the NEWLIST (or the first NEWLIST in case of a MERGELIST).

You can also create and use your own XSLT stylesheet. The stylesheet must be in EBCDIC format. The <xsl:stylesheet> and </xsl:stylesheet> elements must be on separate lines and be the only elements on those lines.

XML_STYLESHEET=NO turns off generating the processing instruction.

If XML_STYLESHEET=IMBED is specified, no DTD will be generated. In this case, XML_DTD cannot be specified. See option XML_DTD. By default, no xml-stylesheet processing instruction will be generated.

Examples

The following is an example to create a RACF user report on z/OS UNIX, which links to an XSLT stylesheet. The allocation is done using alloc type=output, but could have also been done using other allocation, JCL for example.

```
alloc type=racf backup active

alloc type=output dd=auditrpt,
   path='/u/reports/user-special-report-dd060717.xml'
```

```
fileoption dd=auditrpt encoding=UTF-8 fileformat=XML xml_datadict,
   xml_stylesheet=uri("http://publib.boulder.ibm.com/infocenter/tivihelp
            v2r1/topic/com.ibm.zsecure.doc_1.12/c2rxsl01.xsl")

newlist type=racf dd=auditrpt name=userrpt
   select class=user segment=base special
   sortlist key(8) pgmrname revoke(1,hb) revoke_inactive(1,hb),
      restricted(1,hb) protected(1,hb)
```

This example creates an SMF report. It uses an imbedded stylesheet.

```
alloc type=smf active
alloc type=ckfreeze dsn=SYSAPPL.DAILY.CKFREEZE

alloc type=output dd=auditrpt,
   path='/u/reports/smf-special-report-dd060717.xml'
fileoption dd=auditrpt encoding=UTF-8 fileformat=XML xml_datadict,
   xml_stylesheet=imbed(m=c2rxsl01)

newlist type=smf dd=auditrpt name=smfrpt
   select userid:special
   sortlist datetime recorddesc
```

IMBED / INCLUDE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the IMBED or INCLUDE command for running commands from a different source than the source specified by the program or command parameters, and the SYSIN file. The INCLUDE commands can be nested. That is, the input commands can contain another INCLUDE command. The main use of this command is to include sample or user-defined members; this can be used to share queries or output displays. Using the INCLUDE command to include a standard installation-defined member is a simple customization option.

The commands are read immediately after the INCLUDE statement ends. After the secondary input source has been exhausted, processing of the original input source is resumed at the token that terminated the INCLUDE statement. The input listing clearly shows the origin of the input commands.

The parameters are:

ddname= *file*
DD=*file* **FILE=***file*
F=*file*
To imbed the contents of a sequential file or (in combination with the MEMBER parameter) to denote the file containing the member to be imbedded. If MEMBER is specified as well, a partitioned data set (concatenation) must be allocated to the file. This parameter is mutually exclusive with the PATH and FILEDESC parameters.

ESM= *list*
This parameter can contain one name or a list of names of External Security Manager systems. The program only imbeds the file if one of the ESMs mentioned is present on the system running the CARLa.

FILEDESC= *number*
To imbed the contents of an already opened input file. When running the program in a UNIX environment, file descriptor 0 is already processed instead

of SYSIN. It is most useful for passing commands between processes through a pipe. This parameter is mutually exclusive with DD, MEM, PATH.

LICENSE= *list*
This parameter can be used to perform the imbed only if any of the products in the list is currently installed and not disabled through IFAPRDxx. Typically, this parameter is used to prevent syntax errors for non-full-function products.

MEMBER= *name*
MEM=*name*
To imbed the contents of a PDS member. If the ddname parameter is also present, the PDS allocated to that file is used. If the ddname parameter is omitted, the DDname CKRCARLA is assumed. On VM/CMS, the filename allocated to the indicated or defaulted FILEDEF is checked. If it is ISPNULL, the filename is replaced by the indicated MEMBER using the filetype and filemode from the FILEDEF. This behavior is consistent with ISPF use of FILEDEFs for ISPF libraries of the type 'set of CMS files'. This parameter is mutually exclusive with the PATH and FILEDESC parameters.

MARGINS=(*nn,ll***)**
MARGINS(*nn,ll***)**
Set the margins for the included file or member. The default is (1,72) for RECFM=F(B),LRECL=80 input files, and the whole line otherwise.

N
NOLIST
Do not give a listing of the member to be included. This setting propagates down to lower level includes.

NODUP
This parameter can be used to prevent the program from imbedding the same member or sequential file twice (Which can lead to syntax errors). It is not supported for the PATH or FILEDESC method of specifying imbed files.

PATH=' *path/file***'**
To imbed the contents of a UNIX file. The quotations are required. The path and filename are case sensitive. This parameter is mutually exclusive with DD, MEM, FILEDESC

ISPFVAR= *name*
VAR=*name*
V=*name*
To imbed the contents of an ISPF variable. The variable must be present in any of the ISPF variable pools (implicit, shared, profile). If the variable cannot be found, an error message is issued.

LIMIT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The limit command can be used to set limits on execution or number of error messages. LIMIT may be abbreviated to LIM. This command is not supported in restricted mode.

FOCUS= focus | (focus, focus, ...)
This reduces the functionality of the CKRCARLA program to the product code indicated. This is used by zSecure Alert to make sure its workload is attributed to the right product.

Table 295 lists the available product codes with the corresponding product for each code.

Table 295. Supported product codes

ALERTRACF	zSecure Alert for RACF
AUDITRACF	zSecure Audit for RACF
TCIMRACF	Tivoli Compliance Insight Manager Enabler for z/OS RACF
TCIMCICS	Tivoli Compliance Insight Manager Enabler for CICS
TCIMDB2	Tivoli Compliance Insight Manager Enable for DB2
ADMINRACF	zSecure Admin
zsecure_visual_s	zSecure Visual

The default focus is all of the table above except the product codes starting with ALERT. These have to be specified explicitly to be used.

IN= *nn*
I=*nn*
For RACF complexes, this parameter causes input from the RACF database to stop after the specified number of profiles and segments has been read from the RACF database. This parameter is meant for testing purposes to improve response time, e.g. when testing a new report layout. This parameter does not limit the number of SMF records read, use the LIMIT SMFIN=*nn* parameter.

OUT= *nn*
O=*nnn*
For RACF complexes, this parameter causes input from the RACF database to stop after the specified number of profiles and segments has been selected from the RACF database by the outer level SELECT/EXCLUDE parameters. This parameter was originally meant for testing purposes to improve response time, for example, when testing a new report layout. The difference with the NEWLIST OUTLIM= parameter is that LIMIT OUT= has repercussions for all NEWLIST, verify, and report commands that use security database input, while NEWLIST OUTLIM= is limited in effect to the specific NEWLIST. In general, we recommend using NEWLIST OUTLIM= instead of LIMIT OUT= unless you are stress-testing the product's capability to cope with missing security definitions.

ABEND
To cause an abend on certain severity 20 error conditions. Only use this at the request of IBM software support.

MSG= *nn*
M=*nnn*
To set a limit on the number of error messages for a specific volume serial or catalog. The default is 50. If there are more messages than this limit for a specific volume serial or catalog, the surplus is suppressed.

GENERIC
To limit the output of the commands REPORT and (RE)MOVE with the options NONREDUNDANT and REDUNDANT to generic profiles only.

DISCRETE
To limit the output of the commands REPORT and (RE)MOVE with the options NONREDUNDANT and REDUNDANT to discrete profiles only.

ID= *id*
To limit messages and reports to lines concerning a specific user or group. This option merely reduces output, not the processing time. Often SELECT QUAL= is a better choice.

SMFIN= *nn*
To stop reading SMF after the specified number of records has been read.

The LIMIT command is used outside the context of a NEWLIST command. The SMFIN, LIMIT command is used with the NEWLIST TYPE=SMF to limit the amount of SMF records read. For a usage example, see "Example: limit smfin" on page 790.

SMFDD= *number*
Specifies the maximum number of DD names that are used for SMF. The default value of 100 supports previous releases; the maximum number is 1036. The SMFDD=*number* limit is typically used in conjunction with ALLOC DSNPREF=*prefix*, which processes multiple data sets by using one command. If you specify a large maximum number of DD names for SMFDD, be sure to specify a large REGION size in the job step. An error message is generated if the REGION value is too small.

INDEXBIAS=[2 | *nn*]
This parameter can be used to influence the heuristic algorithm that decides whether to switch from indexed I/O to multi-track sequential I/O while reading a data set of a RACF database.

With an index bias of 1 the switch to sequential I/O is done if the number of queued RBA requests exceeds the number of I/O operations necessary to read the whole RACF data set. This is called the index cutoff point.

With bias 2 this cutoff point is the double number of requests. Generally this is expected to increase CPU and I/O for queries that will switch anyway, but will decrease CPU for queries that did not really need to be switched performance-wise. With bias 3 the cutoff point is three times the number of requests, and so on.

The default is 2. Sequential I/O can be favored by setting LIMIT INDEXBIAS=1 in the preamble. Indexed I/O can be further favored by specifying LIMIT INDEXBIAS=3 or more. Sequential I/O can be enforced by SUPPRESS INDEX (see "SUPPRESS INDEX" on page 936). Indexed I/O can be enforced whenever possible with SUPPRESS INDEXCUTOFF (see "SUPPRESS INDEXCUTOFF" on page 936).

The specification has no effect when BDAMQSAM has been specified.

Example - limit discrete

To remove redundant discrete profiles but not redundant generic profiles, the scope of the REMOVE REDUNDANT command can be restricted to discretes by the following command sequence.

```
remove redundant
limit discrete
```

Example - limit msg

You may not see all detail error messages resulting from a VERIFY command on the first run, because of the default message limit of 50 messages per volume. If this is the case, you receive the message:

```
CKR091I volser message limit exceeded- nn messages suppressed
```

To see all detail messages, the message limit should be increased. This can be accomplished by setting it to a sufficiently high value (at least the current limit plus the amount of messages suppressed according to the message). For instance:

```
limit msg=1000
```

Example: limit smfin

```
/* Read at most 10,000 SMF records */
limit smfin=10000
```

When the input limit has been reached, Security zSecure terminates reading of the SMF input files. The remaining records in the input files are not read and cannot be selected, listed or unloaded.

This option is mainly of use in case of response time or memory use problems. To restrict the number of records displayed for any single report, use the OUTLIM parameter of the NEWLIST command. Security zSecure terminates reading the SMF input files if all output limits have been reached.

LANGUAGE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

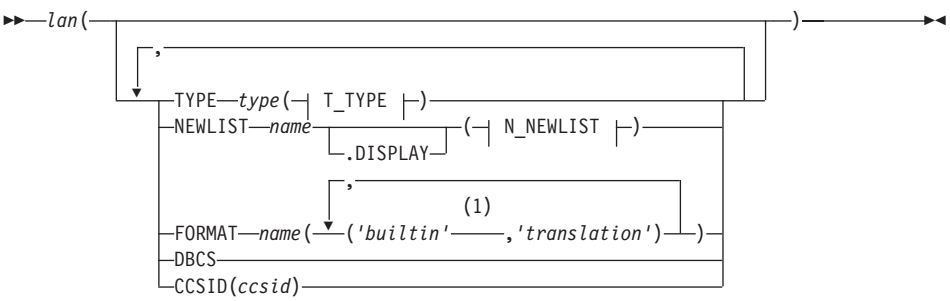
The LANGUAGE command provides the specification for translating CARLa NEWLIST reporting elements and activates translation for certain named NEWLIST types (reports). The LANGUAGE command cannot be abbreviated.

When generating reports, all LANGUAGE commands must precede the use of any NEWLIST statement or field names in the command input stream. Multiple LANGUAGE commands for the same language (lan) can be coded in a single report generation. However, all commands must refer to the same language. For example, you cannot submit commands for LANGUAGE JPN and LANGUAGE KOR in the same report.

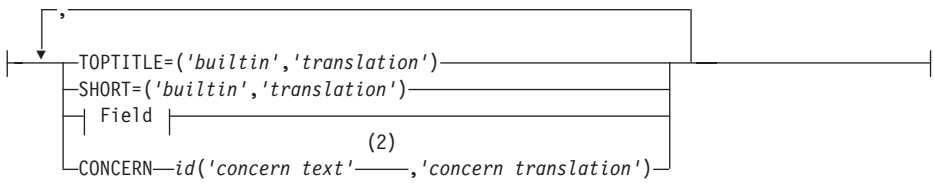
If duplicate parameters are located on subsequent LANGUAGE commands, the last value read from the input takes precedence.

The format of the LANGUAGE command is shown in the following syntax diagram:

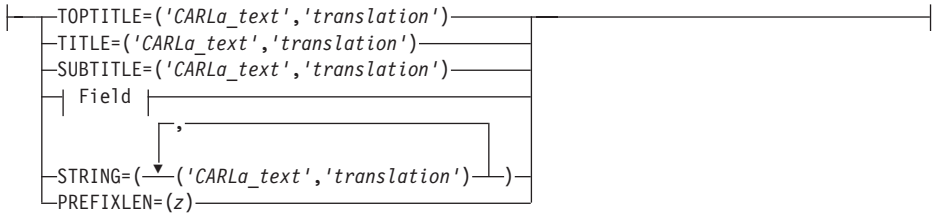
Language



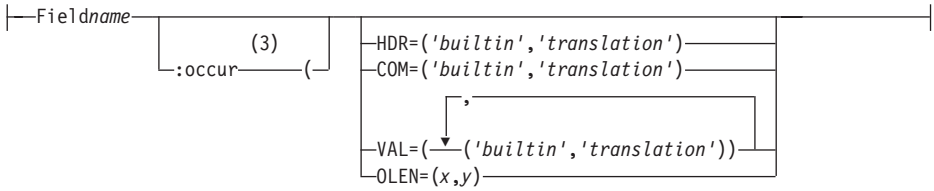
T_TYPE:



N_NEWLIST:



Field:



Notes:

1 The quotations shown around the strings 'builtin' and 'translation' are required. You can use three types of quotation marks: the single quote ('), a double quote ("), and a backquote (`).

2 The strings 'concern text' and 'concern translation' can contain one or more `&variables`,

3 Occurrence number `:occur` is only valid on `FIELD` command under NEWLIST, not under TYPE.

Field descriptions

lan

A three-character code that identifies the translation language.

CCSID (*ccsid***)**

Enter the CCSID of the language being processed (optional). This value is not currently used, but can be provided in case it is needed later.

DBCS

Indicates if the translation language is a DBCS language. This setting controls the following processing behavior:

- Default NEWLIST headers are printed in *asis* format and not interspersed with blanks to make them wider.
- Selecting and excluding using the string scan operator =: uses a DBCS-enabled scan function. Non-DBCS search arguments are not found in DBCS sections of the string, while DBCS search arguments are found only in DBCS sections.

Note: The search results are unpredictable if the string has any invalid DBCS section, binary data that has a stray X'0E') for example.

FORMAT name(('*builtin***','***translation***') [,('***builtin***','***translation***')]...)**

The FORMAT strings are to be translated from the string variable *builtin* to the string variable *translation*. The *builtin* ,*translation* pair can be repeated as many times as required. For example, strings like YES and NO might be translated in a single statement.

NEWLIST name | name.display

This phrase indicates that parameters that follow in parentheses are to be used as the translation instruction for a `NEWLIST NAME=name` statement. Besides giving the translation for this language, this clause also activates actual translation for the indicated NEWLIST. For a DISPLAY statement the name used in `NEWLIST NAME=name` must be suffixed with `.display` in the LANGUAGE NEWLIST clause to disambiguate a display format NEWLIST from the print format NEWLIST with the same name.

FIELD name [:occur]
The field name and optional occurrence number of the NEWLIST field that the language translation applies to.

COM=('*CARLa_text***','***translation***')**
The PREFIX header (field label) of *CARLa_text* for the `FIELD name` is to be translated to the string translation.

HDR=('*CARLa_text***','***translation***')**
The Column Header string of *CARLa_text* for the `FIELD name` is to be translated to the string translation.

OLEN=(*x,y***)**
The output length (column width) of the FIELD name has to be changed from the `actuallength` x, to the `translationlength` y.

VAL=(('*CARLa_text***','***translation***') [,('***CARLa_text***','***translation***')]...)**
The value strings associated with the field name are to be translated from

the string builtin to the string translation. The (*'CARLa_text '*,*'translation'*) pair can be repeated as many times as required.

PREFIXLEN=(x)
Overrides the default PREFIX header (field label) length of 29 for translations where the length is longer than 29. Valid values are 29 to 70 inclusive.

STRING=('*CARLa_text***','***translation***')**
The String value of *CARLa_text* for the FIELD name is to be translated to the string translation.

SUBTITLE=('*CARLa_text***','***translation***')**
Indicates the SUBTITLE string of *CARLa_text* in the NEWLIST name is to be translated to the string translation.

TITLE=('*CARLa_text***','***translation***')**
Indicates the TITLE string of *CARLa_text* in the NEWLIST name is to be translated to the string translation.

TOPTITLE=('*CARLa_text***','***translation***')**
Indicates the TOPTITLE string of *CARLa_text* in the NEWLIST name is to be translated to the string translation.

TYPE *type*

The TYPE=*type* command indicates that the parameters that follow are the default translation for a `NEWLIST TYPE=TYPE`. By itself, this clause does not activate the actual translation. The translation is activated by the `NEWLIST name` clause of the LANGUAGE statement or by the `LANGUAGE=` parameter on the NEWLIST statement.

The TYPE command supports the following parameters.

CONCERN id('*builtin***','***translation***')**
This parameter indicates that the default CONCERN with ID *id* and string *builtin* is to be translated to the string translation.

Variables are presented by ampersand (&) and end with a period (.), for example `&1.`. The translated string can use variables in a different order and put them in a different position in the string.

FIELD *name*
The field name associated with the NEWLIST type that the language translation applies to.

Note: The `FIELD` *name* clause for the TYPE NEWLIST does not support the `:occur` option for specifying the NEWLIST field occurrence number. This option is supported on the `FIELD` *name* clause for the LANGUAGE statement.

COM=('*builtin***','***translation***')**
The PREFIX header (field label) of *builtin* for the `FIELD name` is to be translated to the string translation.

HDR=('*builtin***','***translation***')**
The Column Header string of *builtin* for the `FIELD name` is to be translated to the string translation.

OLEN=(*x,y***)**
The output length (column width) of the FIELD name has to be changed from the *actual length x*, to the *translation length y*.

VAL=(('*builtin*','*translation*'**) [,(**'*CARLa_text*','*translation*'**)]...)**
The value strings associated with the field name are to be translated from the string builtin to the string translation. The ('*builtin*','*translation*') pair can be repeated as many times as required.

SHORT=('*builtin*','*translation*'**)**
This field is not implemented.

TOPTITLE=('*builtin*','*translation*'**)**
Indicates the default TOPTITLE string of *builtin* for the NEWLIST type is to be translated to the string translation.

LIST family of commands

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The **LIST** commands request formatted output of the profile records selected using the **SELECT** and **EXCLUDE** commands. Output is sent to the destination specified using the **PRINT** or **NEWLIST** command. The destination can be a SYSPRINT file or other output destination such as an ISPF display. These commands have a similar syntax. For each selected profile, the fields specified as parameters in the LIST command are list. For information about different output files or simultaneous multiple reports, see the NEWLIST command. Table 296 shows the commands included in the LIST family.

Table 296. LIST family of commands

Command	Description	Sorted	Headers
LIST	Output to file	No	Page headers
SORTLIST	Output to file	Yes	Page and Column headers, if output to SYSPRINT/CKREPORT
DISPLAY	ISPF table	Yes	ISPF
SUMMARY	Summary report	Yes	Page and Column headers, if output to SYSPRINT/CKREPORT
DSUMMARY	ISPF summary table	Yes	ISPF

Note that the LIST command behaves differently from the other commands from this family, in that it generates output for each record at the moment that record is read. This has the advantages of a reduced need for storage and a slightly higher speed. It has the significant disadvantage that nothing is kept in storage, which implies that post-processing is impossible. Several NEWLIST and OPTION parameters suffer from this restriction, which is not always obvious. For this reason, use the LIST command only if strictly necessary.

Note that the DISPLAY command behaves like the SORTLIST command when not in ISPF. When the SUMMARY command is combined with a DISPLAY command, it behaves like DSUMMARY.

If you want to use the (SORT)LIST command for TSO command generation, you may want to suppress page headers. Use the PRINT NOPAGE or NEWLIST NOPAGE command to do so.

The LIST command is not supported in restricted mode for NEWLIST TYPE=RACF (the default list type), but the SORTLIST and DISPLAY commands are supported. Some fields cannot be used on the LIST command, notably the ACL field.

Details on the LIST family of commands describe report and display options, output formatting, and other processing that applies to these commands. For additional information about LIST family commands other than the LIST command, see the following sections:

- "DSUMMARY" on page 778
- "SORTLIST" on page 918
- "SUMMARY" on page 918

Controlling report and display output for LIST family commands

CARLa provides a number of parameters to control report display and output using the LIST family of commands. These parameters include output modifiers and format names. The following sections describe how zSecure report and display processing works and explains how to use the output modifiers and format names to control the behavior and appearance of display and report output.

Note that not all modifiers and formats are available for all commands and that different modifiers and formats are available based on field type (repeat group, non-repeat group, flag, and date fields, for example). These sections also include examples of using the output and format modifiers. Additional examples are provided in "Using the LIST command" on page 832

- "Repeat groups and repeated fields: Understanding the output list processing" on page 796
- "Parameter syntax: Specifying parameters for LIST/SORTLIST/DISPLAY commands" on page 796
- "Indirect references: Using lookup" on page 796
- "Modifying output length" on page 797
- "Modifying output format" on page 798
- "General output modifiers: Controlling field-related output" on page 798
- "Display modifiers: Changing field output display in ISPF" on page 802
- "Non-repeated field output modifiers: Changing how information is displayed" on page 803
- "Repeated field output modifiers: Changing display of Repeated fields" on page 804
- "Summary statistic modifiers: Changing the output display for SUMMARY operations" on page 809
- "Modifying the column header" on page 809
- "Changing the sort order" on page 809
- "Format names for input and output" on page 810
- "Specifying syntax for RACF command input" on page 810
- "Flag formats: Using available formats for flag field input and ouput" on page 826
- "Date output formats: Formatting date field output for different locales and standards" on page 828

Repeat groups and repeated fields: Understanding the output list processing

If the field is part of a repeat group, the listing contains as many lines as necessary to list all member values in a column. If two fields are displayed that are part of the same repeat group such as the ACL fields `USERACS` and `USERID`, the corresponding repeat group values appear on the same line unless one of the columns contains the SORT format modifier.

If the output listing contains one or more repeat group fields (profile key, for example), the first line contains all non-repeat group fields and the first value of each repeat group field. All fields that are not part of a repeat group are blank in subsequent lines unless the RETAIN parameter was specified on theOPTION or NEWLIST command.

Parameter syntax: Specifying parameters for LIST/SORTLIST/ DISPLAY commands

The parameters to the LIST/SORTLIST/DISPLAY commands must either be:

- *strings* enclosed in single, double, or left quotations, with a maximum length of 512 characters.
- For `NEWLIST TYPE=RACF`, field names as defined by the templates ("TEMPLATE - Template field properties" on page 284) or built-in *pseudo-fields*. For other NEWLIST types, pre-defined *field names* as defined in this manual. All fields available are described in SELECT/LIST fields.
- Boolean, summary, or subselect *variables* defined with the DEFINE command (see "DEFINE" on page 750).
- *indirect references* (also called *lookup*) as described in "Indirect reference or lookup" on page 764.
- the *concatenation operator* `'|'` (a vertical bar).
- the *newline operator* `'/'` (a slash).
- the *soft newline operator* `/n` (valid on the following commands: `SORT`, `SORTLIST` and `SUMMARY` only)

In addition, the `DSUMMARY` and `SUMMARY` commands support the following syntax:

- the *summary level operator* `*` (an asterisk).
- The parameters can be separated by blanks or commas. If the statement needs to be continued on the next line, the last parameter on the line must be followed by a comma.
- The parameters containing field names (or their aliases) can be immediately followed by a list of *output modifiers* enclosed in parentheses.

  The output modifiers are: length, format, repeat group format modifiers, non-repeat group modifiers, general format modifiers, and an overriding column header. An output field can be specified using the following syntax. For additional information, see "Modifying output format" on page 798.

  ```
  fieldname
  fieldname:reference
  fieldname(length,format,modifier,'header',...)
  ```

  Note: The concatenation, newline, and summary level operators must be separated from parameters by either blanks or commas.

Indirect references: Using lookup

Indirect references (also called *lookup*) are fully described in "Indirect reference or lookup" on page 764.

Note that for a NEWLIST TYPE=RACF, the LIST command does not support indirect references.

If the base field name is not present separately in the output command, it is automatically inserted before the look-up field, and it receives the NONDISPLAY output modifier. Note that this can influence the sort order. If you want to sort on the lookup field, make that the base field is present in the output command *behind* the look-up field. You may use the NONDISPLAY output modifier if you do not want the base field to be present in the output.

For the use of indirect references in the summary, see "Indirect references in a summary" on page 926.

Modifying output length

Optionally, a field name may be followed by a *length* in parentheses. This number indicates the number of output positions into which the field should be formatted. Most fields have default lengths predefined that are sufficient for standard usage. If the NEWLIST TYPE=RACF field is defined as a variable length field in the template *and* no default length is set by Security zSecure (this is listed on the SHOW TEMPLATES output) *and* no explicit length is provided on the LIST command, the actual length is used for each profile. This results in disturbance of the column layout, because all subsequent fields start at a varying position.

The overriding output length 0 has a special meaning, dependent on the command issued. For the DISPLAY command it can only be used on the last field on a line. If the output field is not modifiable, it will then use all remaining space on the line on the screen. A modifiable field will allocate the maximum input length supported for the field or its output format. This may require many scroll-right operations to reach the end of the field for, e.g., a maximum input length of 1023. If WRAP is also specified, the field will wrap at end of screen - but only if the current contents are longer than fits on the screen (no right scrolling is required in this case). If the current contents fit on the screen in the first line, but the field maximum length is longer than fits on the screen, WRAP will cause the field to be extended just to the end of the screen but not generate continuation lines - this means that the maximum input length cannot necessarily be entered when WRAP has been specified. For the (SORT)LIST command it means that trailing blanks must be trimmed (stripped) from the output. It generally results in a ragged column layout, but can be used to generate your own TSO commands. The following example will put quotations around a profile key.

```
sortlist "'" | key(0) | "'"
```

With a (D)SUMMARY command, an overriding output length has a special meaning. The summary will be done after recalculating the value off the field to match the specified length. For example, in the following code data is summarized on the first four characters of the user ID. An overriding length of zero on a (D)SUMMARY command thus generates no useful output.

```
select class=user segment=base
sortlist key owner name
summary key(4)
```

Instead of defining length values using numerals, you can use the SYMBOLIC statement (`SYMBOLIC NUM name=value`) to define a symbolic name for a numeric value. The symbolic name can be used on its own or associated with a numeric default value that is used if the symbolic has not been defined. The default value is specified as `name|value` as shown in the following examples: "SYMBOLIC" on page 940.

```
SELECT NUMBERFIELD>maxlength
SELECT NUMBERFIELD>maxlength|20
```

In the CARLa command input, the symbolic name must be defined before its first use. If you use the conditional specification, the value is the default value that is used only if the SYMBOLIC statement has not been defined. For more information and usage restrictions, see "SYMBOLIC" on page 940.

Modifying output format

Instead of the length, or in addition to it, a *format* can be defined. An output format changes the way a field is displayed. Generally this is unnecessary, but it may for instance be used to display dates in US format, to print a suspect value in hexadecimal, or to generate TSO commands. The output formats that can be specified are described under "Specifying syntax for RACF command input" on page 810. This section includes a list of special output formats starting with a **$** that are used to generate TSO commands.

General output modifiers: Controlling field-related output

General output modifiers are available to change the way a field appears or behaves in reports and displays and to control aspects of the report output such as changing the page title to include the field value. General output modifiers use the same syntax as output formats, in parentheses following a field name (`fieldname(INDENT(indent_fieldname)`). A field can have both general output modifiers and output formats specified together. and can be included in addition to output formats. They apply to both repeated and non-repeated fields. The following general output modifiers are provided:

ALLOWRESTRICT
: Allow a restricted field in a query in restricted mode. Messages CKR0217 and CKR0384 are still issued, but with severity 4 (warning) instead of 12 (syntax error). The resulting report will be generated with an empty column for the restricted field. If you want to allow this for all fields in the query, use the ALLOWRESTRICT modifier on the NEWLIST command. If you want to suppress an entire query in restricted mode rather, use the UNRESTRICTED modifier on the NEWLIST command. See "OPTION" on page 856.

BOTH
FIRST
: This modifier has effect on ISPF displays only. It specifies that the field should be shown on both the overview and the detail panel. For a repeated field, the first value will be shown on the overview panel, unless the repeat group modifier MORE is also specified. This modifier is mutually exclusive with DETAIL and NODETAIL. It is subordinate to NONDISPL.

CONDPAGE(nnn)
CP(nnn)
: The CONDPAGE modifier can be used to force the start of a new page in a report that is written to file if there are not enough lines left on the current page to print a section. The number specified between parentheses is the minimum number of lines needed on the current page. If there are less lines than specified left, a new page is started. Any number between 1 and 255 can be specified and the modifier can only be used on the first field or string on a line.

DESCENDING
BW
: Reverses the sort order for this column. Note that this is used to sort *records*, not repeated field instances. When used on a repeated field, the record sort

order for this column is descending for the first repeated field instance. Use the SORT(DESCENDING) output modifier to change the sort order within a repeated field.

DETAIL
D

This modifier has effect on ISPF displays only. It specifies that the field should be shown on the detail panel, and not on the overview panel. This modifier is mutually exclusive with BOTH and NODETAIL. It is subordinate to NONDISPL. Its effect can also be specified as default for all fields with the NEWLIST option DETAIL. Note that a DISPLAY command must show output on the overview panel.

INDENT

Displays the field with an indentation determined by the parameter to INDENT, which must be a numeric (one to four byte integer) field to the right of the indented field on the same command (and level, for a summary).

The syntax of the INDENT output modifier is:

```
fieldname(INDENT(indent_fieldname))

fieldname          any field name
indent_fieldname   any field name that has a numeric value
```

This modifier is useful in a group-tree display where `KEY(40,INDENT(DEPTH))` displays each group name in a 40 character wide column. Each group name is prefixed by blanks to indicate the depth within the group tree. If a repeated field is indented by a non-repeated field or a repeated field with the FIRSTONLY modifier, each entry of the repeated field is indented by the non-repeated field value. If a repeated field is indented by another repeated field, the first entry of the former is indented by the first of the latter, the second by the second, and so on. A missing value results in no indentation. The `INDENT` setting is a print phase modifier, which means that the prefixed blanks are not used for sorting or summarizing. Do not combine indenting a repeated field by another repeated field with a `SORT`, `WRAP` or `WORDWRAP` modifier or with the `DUMP` output format on either field. This type of combination produces confusing report formatting.

KEY

On an ISPF display, the field is a *key field*. When scrolling left/right, the key fields always remain on the display. That is, only the non-key fields are scrolled left and right. Key fields must be adjacent. You cannot have a key field followed by a non-key field followed by a key field.

NOMODIFY

Set the field to non-modifiable. This is only of use in ISPF displays. This parameter overrides the NEWLIST setting.

NODETAIL

This modifier has effect on ISPF displays only. It specifies that the field should be shown on the overview panel, and not on the detail panel. For a repeated field, the first value will be shown on the overview panel, unless the repeat group modifier MORE is also specified. This modifier is mutually exclusive with BOTH and DETAIL. It is subordinate to NONDISPL.

NONDISPL
NONDISPLAY

ND
Do not display / list the value for this field. This is useful for changing the sort order without having to display the sort key (in that specific position or anywhere), or to hide a summary key.

NOPREFIX
Locally override a NEWLIST HEADER=PREFIX and in this way suppress the 30 character field comment prefix.

NOSORTLIST
This modifier can be used to exclude a column from the record sort key. The record sort key consists of the fields listed in the output specification (for example SORTLIST, SUMMARY). As an alternative to using the NOSORTLIST output modifier, you can also explicitly specify the sort key through the list of fields by using the NONDISPLAY output modifier, as shown in the following examples:

```
Display key(8,NOSORTLIST) pgmrname(NOSORTLIST) owner

Display owner(NONDISPLAY) key(8) pgmrname owner
```

Using "field(nosortlist)" usually leads to shorter and simpler CARLa statements. Using "field(nondisplay)" has the benefit of requiring less CPU time than "field(nosortlist)" to create similar output.

NOTEMPTY
NE
The NOTEMPTY modifier can be used to suppress the line it is issued on when all fields on it are empty. The modifier can only be used on the first field or string on a line and works only for a report that is written to file, not for an ISPF display.

PAGE
This modifier causes a page eject if the value of the field changes. It does not effect the output position of the field, add TOPTITLE if the field must be displayed as a running variable in the header. More than one field can have the page modifier but they must be concentrated at the beginning of the sortlist statement. The only columns supported on the statement before a field with a PAGE modifier are string literals and newlines. The PAGE modifier cannot work on a LIST statement.

PREFIX
P This modifier specifies that the field value should be prefixed with a descriptive text (a *prefix header*) of 29 characters followed by one blank as a separator. The *prefix header* is generally different from the *column header*, because columns are usually narrow. PREFIX can be specified for all fields at the same time by using the parameter HEADER=PREFIX on an OPTION or NEWLIST statement.

TITLE
T This modifier causes the field to be printed behind the default or explicitly specified title. It is not printed on the regular output line, TOPTITLE and TITLE fields can be freely mixed (have an arbitrary order), but they must come before any fields on the statement that do not have any of the modifiers TITLE, TOPTITLE, or NONDISPL. TOPTITLE and TITLE are mutually exclusive. The TITLE modifier cannot work on a LIST statement. If a repeated field has this modifier, then only the first value is displayed. Title fields start immediately behind any specified NEWLIST TITLE='string' without intervening blanks.

TOPTITLE
TT

This modifier causes the field to be printed behind the default or explicitly specified toptitle. It is not printed on the regular output line. TOPTITLE and TITLE fields can be freely mixed (have an arbitrary order), but they must come before any fields on the statement that do not have any of the modifiers TITLE, TOPTITLE, or NONDISPL. TOPTITLE and TITLE are mutually exclusive. The TOPTITLE modifier cannot work on a LIST statement. If a repeated field has this modifier, then only the first value is displayed. Title fields start immediately behind any specified NEWLIST TOPTITLE='string' without intervening blanks. Specifying any TOPTITLE modifier in the NEWLIST suppresses the automatic display of variables like time stamps and BUNDLEBY variables on the top title, these can be displayed by adding the STAMP field and the bundle variable to the SORTLIST with a TOPTILE modifier.

TRUNCATE
TRUNC

This modifier causes error and warning messages CKR0397 and CKR0218 to be suppressed if the field exceeds the line length or starts beyond end of line.

VARLEN

Force the field to be treated as variable length. This is useful for fields that are automatically treated as fixed length, but then cause message CKR1968 to be issued.

The CKR1968 usually signals an error condition in the database, where the templates indicate the field is fixed length, but there are values in the database that are out of spec. You can look for the erroneous values with the following query:

```
define fieldname(VARLEN) as fieldname
newlist type=racf
display class key segment fieldname(dump)
sum fieldname(fldlen,'Len')
```

The *fieldname* indicated in the CKR1968 message should be substituted. In the resulting summary, look for entries with a length different from 0 and the *expected* length indicated in the message.

If it turns out some field values in the live database are indeed incorrect, you can write a CARLa query to select the offending records and generate corrective RACF or CKGRACF commands for them.

If you want to permanently circumvent (rather than fix) the problem, you can put the DEFINE statement in your PREAMBLE, or in CARLa member C2RXDEFU (which is automatically included in the interface and several sample batch jobs).

UNIVERSAL

This modifier requests to show (access for, the number of) all connects to groups with the UNIVERSAL attribute. It can be used with the ACL, CONNECTS and CONNECT_COUNT fields.

A group without the UNIVERSAL attribute can have at most 5957 connected users, due to a size limit on the list of connected users in the group profile. The UNIVERSAL attribute removes this restriction, as the group profile for a universal group does not list users connected with just USE authority (and no connect attributes like group-special) in the ACLCNT repeat group.

These relatively uninteresting connects are only shown in the ACL, CONNECTS and CONNECT_COUNT pseudo-fields, when the UNIVERSAL modifier has been specified. Note that this may increase the response time of your query, because all user profiles in the database must be examined for a possible connect to the universal group (indexed I/O is disabled).

For the ACL field, this modifier also controls whether access due to system operations may be shown (depending on the other ACL modifiers used), another function that requires all USER profiles to be examined.

WORDWRAP
WW

The WORDWRAP modifier is like the WRAP modifier, except that it splits the line at a word boundary (`=blank`) instead of splitting words across lines. However, if a word is longer than the column is wide, then it forces a split across lines. With this setting, processing does not suppress blanks at that occur at the beginning of a new line.

When a field in a `DISPLAY` statement is specified with the `WORDWRAP` modifier, the field is shown in the Detail ISPF display panel but not in the Overview display panel.

WRAP
W

The `WRAP` modifier without the `HORIZONTAL` setting wraps a field value in the column if it is too wide for the column. This format effectively creates a repeat group display for each value of the field where each subsequent line in the column continues the text of the previous line. If an output length of *0* is specified or implied, the rest of the line is used as the width of the column to wrap in. For output format `HEX*`, an odd column width is supported. The `(WRAP,HEX,0)` specification automatically rounds down to a byte boundary (even width), except for width 1.

`WRAP` is not supported in combination with the following output formats: `HDR$BLANK`, `BLANK$HDR`, `STR$BLANK`, `BLANK$STR`, and `DATE$STR`. If the `HORIZONTAL` modifier is specified for the same field, `WRAP` acts as a secondary modifier to `HORIZONTAL`, see "Repeated field output modifiers: Changing display of Repeated fields" on page 804.

When a field in a `DISPLAY` statement is specified with the `WRAP` modifier, the field is shown in the Detail ISPF display panel but not in the Overview display panel.

Display modifiers: Changing field output display in ISPF

To change the color and intensity of a field on an ISPF display *display output modifiers* are available. The display output modifiers can be specified like and in addition to the output formats, in parentheses following a field name. They apply to both repeated and non-repeated fields. The colors mentioned are default values and can be changed by the ISPF settings. The following display output modifiers are provided:

BOLD
B The field is displayed in bold (highlighted). It will be shown highlighted on a monochrome terminal and blue on a color terminal.

CH

The field is a column header. It will be shown highlighted on a monochrome terminal and blue on a color terminal.

CT
The field is caution text. It will be shown highlighted on a monochrome terminal and yellow on a color terminal.

DEFAULT
L
LID
The field is a list detail field. It will be shown normal on a monochrome terminal and green on a color terminal.

ET
The field is enhanced text. It will be shown highlighted on a monochrome terminal and turquoise on a color terminal.

FP
The field is a field prompt. It will be shown normal on a monochrome terminal and green on a color terminal.

LI
The field is a list key. It will be shown highlighted on a monochrome terminal and white on a color terminal.

NT
The field is normal text. It will be shown normal on a monochrome terminal and green on a color terminal.

PAS
The field is a point-and-shoot field. It will be shown highlighted on a monochrome terminal and turquoise on a color terminal. It functions as a push button in the GUI. This modifier is only valid on fields that have the KEY modifier as well.

SI
The field is scroll information. It will be shown highlighted on a monochrome terminal and white on a color terminal.

WASL
The field is a window area separator line. It will be shown normal on a monochrome terminal and blue on a color terminal.

WT
The field is warning text. It will be shown highlighted on a monochrome terminal and red on a color terminal.

Non-repeated field output modifiers: Changing how information is displayed

For non-repeated fields, specific *non-repeated field output modifiers* can be specified to change the way the information is displayed. This is in addition to the output format that can be specified. The non-repeated field modifiers are:

EXPLODE
Turn a condensed non-repeated field into an expanded repeated field. This output modifier can only be used with the FLAG, FLAG2NICE, KEYUSAGE_RACF, KEYUSAGE_X509, LOGDAYS, RESFLG, YESNO, $YESNO, and $NO formats and the zSecure Audit for ACF2 DESCRIPTOR, REASON, and RACFAUTH fields. The EXPLODE output modifier is also used with the ACL repeat group field, see "Repeated field output modifiers: Changing display of Repeated fields" on page 804.

NORETAIN
Locally override a NEWLIST RETAIN to not repeat the value of this non-repeated field for each line.

RETAIN
Repeat a non-repeated field for each line that is needed to list the contents of all repeated fields on the line. This is for instance useful to generate a TSO command for each occurrence in a repeated field. This can also be specified for all fields at the same time by using the NEWLIST parameter RETAIN.

Repeated field output modifiers: Changing display of Repeated fields

For repeated fields, *repeated field output modifiers* can be specified to change the way in which the information is displayed. This is in addition to the output format that can be specified. The repeated field modifiers are:

EFFECTIVE
Reduce the repeated field such that only relevant entries, showing actual access remain; in case access is only granted implicitly, add an explicit entry.

Currently, EFFECTIVE is only valid on the ACL combination field. Applying it results in an access list display showing all user IDs that have access and the actual access they have through any access list entry, or if they have access due to an operations attribute the group in which they have group operations, or `- oper -` for a system-wide operations attribute.

Whether administrative access is also taken into account depends on the SCOPE modifier (see there). System-wide operations and access of users with default connections to a universal group will only be taken into account if the UNIVERSAL modifier is also specified.

Specifying EFFECTIVE will disable indexed read of the RACF database and switch to full read.

EXPLODE
Values in the column that can be expanded must be expanded.

For the ACL combination field, this requests that all groups are to be expanded into the user IDs connected to the group. In addition, operations access is shown as well as access ALTER-O; the ACL id shows `- oper -` for system operations and the group name for group operations. Whether administrative access is also taken into account depends on the SCOPE modifier (see there).

The EXPLODE output modifier is also used to turn some condensed non-repeated fields into expanded repeated fields, see "Non-repeated field output modifiers: Changing how information is displayed" on page 803.

System-wide operations and access of users with default connections to a universal group will only be taken into account if the UNIVERSAL modifier is also specified.

FIRSTONLY
Reduce the repeated field to its first entry. If SORT is specified too, the expectation is that the repeated field is sorted first and then truncated; support for a combination with SORT on a SUMMARY statement is limited. Since the resulting field is no repeated field, FIRSTONLY cannot be combined with MORE.

HEADER
If there is a non-blank value in the field, an extra line is shown before the line containing the field values. The extra line contains the default header for the field. Header is meant to be used for lines containing only one field (column); the result is not defined otherwise. On an ISPF display, the header is shown highlighted. The header is also shown if the field is modifiable and can be used to add a (new) value.

HORIZONTAL(*entrylength***)**
HOR(*entrylength***)**

The values of a repeated field are to be listed horizontally, for example, multiple values are to be shown on a line. Note that the HORIZONTAL modifier applies locally to a field, so it is not possible to horizontally repeat a combination of two fields from the same repeat group; however, each field can be listed horizontally on its own line using HORIZONTAL, while the '/' newline operator can be used to put each field on its own line.

Normally, the output length for a field can be interpreted as either the length of the output column in the report or the length used to print an entry in that column. When HORIZONTAL is specified, the two are no longer equivalent. Therefore, the entry length can be specified separately between brackets. By specifying entry length 0, the entries may be packed as tightly as possible (though still separated by one blank). When HORIZONTAL is specified **with** brackets, but **without** an entry length between the brackets, the default output length of the field is used as the entry length.

If a WRAP or WORDWRAP modifier is specified in addition to HORIZONTAL, the combination indicates that multiple lines can be used, and furthermore WRAP or WORDWRAP is applied to each repeated field value separately. Effectively, this means that a repeat group entry is only added to the same line within the specified column if it fits completely (including any padding implied in the case of a fixed width entry length). If it does not fit, a new line is added to the column and if it still does not fit, it is (word)wrapped to additional lines.

Deprecated syntax: HORIZONTAL can also be specified without brackets. In combination with WRAP this means that the output length specified or implied is used as the column width (as usual). The entry length cannot be specified in the old syntax and defaults to 0 (tight packing).

If a first HORIZONTAL occurs **without** WRAP, the old syntax will interpret the output length up to that point as the *entry* length and the *column* length becomes 0. This is flagged as confusing syntax by informational message CKR1248 (except for explicit length 0).

If a DEFINE statement contains any HORIZONTAL specification without WRAP and a subsequent use of the variable also specifies HORIZONTAL in the old syntax without WRAP, the following occurs. An output length specification updates the *entry* length, the *column* length is not changed and depends on the preceding DEFINE statement. This is flagged as confusing syntax by informational message CKR1249 (unless both column and entry length are 0).

Example - Using HORIZONTAL with a fixed entry length for an easily readable report

This example shows how to produce an easily readable report for the connect groups of each user. Each connect group name is printed in 8 positions (the default output length of CGGRPNM), and the total report has width 78 (though the line length is 80). Only the first 7 connect groups are shown.

```
newlist type=racf ll=80
 select class=user segment=base
 sortlist key(8,"User") cggrpct cggrpnm(hor(),62)
```

This produces output like the following.

```
P R O F I L E   L I S T I N G   12 Sep 2003 00:07                    page    1

User     #Conn ConGroup
C##AHOU      7 C##A     C##ACONF C##ARACF C##B     C##BCCW  C##GRACF RCOPROB1
C##AH02      5 C##A     C##ACONF C##ARACF C##B     C##BCCW
C##AINT     13 C##      C##A     C##AWIN  C##B     C##BEPRD C##BTSUP C##BZDEV
C##AROB     15 C##A     C##ARACF C##B     C##BEPRD C##BOMVS C##BTSUP C##C
C##ARO2     10 C##A     C##ARACF C##B     C##BTSUP C##C     C##CNG   C##CXDEL
C##ASCH     13 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP
C##ASC2      2 C##A     C##GRACF
C##ASC3     10 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP
```

Example - Using HORIZONTAL with column width 0 to fill out the output line

This example shows how to produce an easily readable report for the connect groups of each user. Each entry is printed in 8 positions (the default output length of CGGRPNM). The width of the report depends on the line length (but it is explicitly set to 80 in this case), and as many connect groups are shown as will fit on the line.

```
newlist type=racf ll=80
 select class=user segment=base
 sortlist key(8,"User") cggrpct cggrpnm(hor(),0)
```

Note that column length 0 can be used for the last field on a line to mean the rest of the line.

This produces output like the following.

```
P R O F I L E   L I S T I N G   12 Sep 2003 00:07                    page    1

User     #Conn
C##AHOU      7 C##A     C##ACONF C##ARACF C##B     C##BCCW  C##GRACF RCOPROB1
C##AH02      5 C##A     C##ACONF C##ARACF C##B     C##BCCW
C##AINT     13 C##      C##A     C##AWIN  C##B     C##BEPRD C##BTSUP C##BZDEV CR
C##AROB     15 C##A     C##ARACF C##B     C##BEPRD C##BOMVS C##BTSUP C##C     CR
C##ARO2     10 C##A     C##ARACF C##B     C##BTSUP C##C     C##CNG   C##CXDEL CR
C##ASCH     13 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP CR
C##ASC2      2 C##A     C##GRACF
C##ASC3     10 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP CR
C##ATST      1 C##A
```

Example - Using HORIZONTAL with entry length 0 for compact output

This example shows how to pack as many connect groups for each user as will fit on one line.

```
newlist type=racf ll=80
 select class=user segment=base
 sortlist key(8,"User") cggrpct cggrpnm(hor(0),0)
```

This (preferred) syntax is equivalent to `cggrpnm(hor,0)`.

Note that column length 0 can be used for the last field on a line to mean the rest of the line.

This produces output like the following.

```
P R O F I L E   L I S T I N G   12 Sep 2003 00:07                    page    1

User     #Conn
C##AHOU      7 C##A C##ACONF C##ARACF C##B C##BCCW C##GRACF RCOPROB1
C##AH02      5 C##A C##ACONF C##ARACF C##B C##BCCW
C##AINT     13 C## C##A CRMAWIN C##B C##BEPRD C##BTSUP C##BZDEV C##C C##CNG C##C
C##AROB     15 C##A C##ARACF C##B C##BEPRD C##BOMVS C##BTSUP C##C C##CNG C##CXDE
C##ARO2     10 C##A C##ARACF C##B C##BTSUP C##C C##CNG C##CXDEL C##DELET C##GRAC
C##ASCH     13 C##A C##AAPPC C##ARACF C##B C##BDOC C##BEPRD C##BTSUP C##BZDEV C#
C##ASC2      2 C##A C##GRACF
C##ASC3     10 C##A C##AAPPC C##ARACF C##B C##BDOC C##BEPRD C##BTSUP C##CNG C##C
C##ATST      1 C##A
```

Example - Using HORIZONTAL with WRAP to print a table layout

This example shows how to print all connect groups for each user using multiple lines, in a report of width 78 and with a table-like layout where each entry is printed in 8 positions.

```
newlist type=racf ll=80
 select class=user segment=base
 sortlist key(8,"User") cggrpct cggrpnm(hor(),62,wrap)
```

This produces output like the following.

```
User     #Conn ConGroup
C##AHOU      7 C##A     C##ACONF C##ARACF C##B     C##BCCW  C##GRACF RCOPROB1
C##AH02      5 C##A     C##ACONF C##ARACF C##B     C##BCCW
C##AINT     13 C##      C##A     C##AWIN  C##B     C##BEPRD C##BTSUP C##BZDEV
               C##C     C##CNG   C##CXDEL C##D     C##GRACF C2RADMIN
C##AROB     15 C##A     C##ARACF C##B     C##BEPRD C##BOMVS C##BTSUP C##C
               C##CNG   C##CXDEL C##DTEST C##GRACF C2ESERVG C2RADMIN C2RSERVG
               RCOPROB1
C##ARO2     10 C##A     C##ARACF C##B     C##BTSUP C##C     C##CNG   C##CXDEL
               C##DELET C##GRACF RCOPROB1
C##ASCH     13 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP
               C##BZDEV C##CNG   C##CXGRP C##GRACF C2RADMIN RCOPROB1
C##ASC2      2 C##A     C##GRACF
C##ASC3     10 C##A     C##AAPPC C##ARACF C##B     C##BDOC  C##BEPRD C##BTSUP
               C##CNG   C##CXGRP C##GRACF
C##ATST      1 C##A
```

Example - Using HORIZONTAL with WRAP to print all entries tightly

This example shows how to print all connect groups for each user using as few lines as possible.

```
newlist type=racf ll=80
 select class=user segment=base mask=crma*
 sortlist key(8,"User") cggrpct cggrpnm(hor,wrap,0)
```

This syntax is equivalent to `cggrpnm(hor(0),wrap,0)`.

Note that column length 0 can be used for the last field on a line to mean the rest of the line.

This produces output like the following.

```
P R O F I L E   L I S T I N G   12 Sep 2003 00:07                    page    1

User     #Conn ConGroup
C##AHOU      7 C##A C##ACONF C##ARACF C##B C##BCCW C##GRACF RCOPROB1
C##AH02      5 C##A C##ACONF C##ARACF C##B C##BCCW
C##AINT     13 C## C##A C##AWIN C##B C##BEPRD C##BTSUP C##BZDEV C##C C##CNG
               C##CXDEL C##D C##GRACF C2RADMIN
C##AROB     15 C##A C##ARACF C##B C##BEPRD C##BOMVS C##BTSUP C##C C##CNG
               C##CXDEL C##DTEST C##GRACF C2ESERVG C2RADMIN C2RSERVG RCOPROB1
C##ARO2     10 C##A C##ARACF C##B C##BTSUP C##C C##CNG C##CXDEL C##DELET
               C##GRACF RCOPROB1
C##ASCH     13 C##A C##AAPPC C##ARACF C##B C##BDOC C##BEPRD C##BTSUP C##BZDEV
               C##CNG C##CXGRP C##GRACF C2RADMIN RCOPROB1
C##ASC2      2 C##A C##GRACF
C##ASC3     10 C##A C##AAPPC C##ARACF C##B C@@BDOC C##BEPRD C##BTSUP C##CNG
               C##CXGRP C##GRACF
C##ATST      1 C##A
```

MORE
This modifier has effect on ISPF displays only. It specifies that the overview panel should show the only value for the field in records where it has only one value, but the text '<more>' or '+' when there are more. It furthermore implies that the field should be shown on both the overview and the display panel, unless one of the general output modifiers DETAIL, NODETAIL or NONDISPL has been specified for the field. (Note that the NEWLIST option DETAIL is ignored.) See also general output modifier BOTH.

NODUP
Duplicates in this repeated field must be eliminated. This modifier implies SORT.

NOSCOPE
This modifier is only effective on the ACL field. It negates the effect of a previous SCOPE modifier (e.g, in a DEFINE AS).

RESOLVE
Values in the column that can be expanded must be expanded, and the duplicate entries deleted until one (arbitrary) entry with the highest access remains, unless a specific, non-expanded entry was present. Access through operations or group operations attributes is not shown.

Currently, the only field where RESOLVE is valid is the ACL combination field. This results in an access list display showing all user IDs and the actual access they have through any access list entry.

Whether administrative access is also taken into account depends on the SCOPE modifier (see there). Access of users with default connections to a universal group will only be taken into account if the UNIVERSAL modifier is also specified.

SCOPE
This modifier is only effective on the ACL field. It requests administrative access to be added to the access list display, if also one of the modifiers EXPLODE, RESOLVE, or EFFECTIVE has been specified. The SCOPE modifier adds access list rows for ownership and access through group-special authority as "OWNER" access and authority on the data set qualifier as "QUALOWN" when EXPLODE is in effect, and causes those extra access list entries to participate in the RESOLVE or EFFECTIVE processing.

SORT
The column must be sorted. This is done by ascending internal value, unless a sort modifier is included between parentheses. The SORT modifier is local to the parameter where it is specified. If you want to display more than one field

of a repeat group and sort them, you should use a supported combination field name (e.g. ACL or CONNECT) to access the repeat group as one column, and/or use indirect reference based on the sorted column. The SORT modifier can be further qualified by a *sort order modifier* enclosed in parentheses immediately behind the SORT output modifier. Two sort order modifiers can always be used: ASCENDINGand DESCENDING. The default is ascending sort order. Three other sort order modifiers are valid only for the ACLand CONNECTS combination fields; these are **USER**to sort on user ID (ascending), **ID** to sort on id in the access list (user or group, ascending),and **ACCESS** to sort on access level (from ALTER to NONE). The default sorting for ACL and CONNECTS is USER. Specifying DESCENDING results in ACCESS. Note that using the DESCENDING output modifier by itself (as opposed to SORT(DESCENDING)) will *not* change the sort order within a repeated field, but will change the record sort order.

Summary statistic modifiers: Changing the output display for SUMMARY operations

In addition to output modifiers, the statistics of a summary command can specify *statistic modifiers* to change the way SUMMARY operates. This modifier is valid on fields of the (D)SUMMARY commands as well as on the DEFINE statement.

NOPROP NP
Do not propagate this statistic to higher levels of the (D)SUMMARY command. This can be used to stop the default behavior of automatically propagating all statistics to higher summary levels if they are not present there yet.

>number <number <=number >=number
A relational operator can be used to indicate a *threshold condition* for the statistic. A summary level is only displayed/listed if all thresholds of the statistics at that level are satisfied. The threshold condition only applies to statistic variables with numeric values.

Instead of defining threshold values using numerals, you can use the SYMBOLIC statement (`SYMBOLIC NUM name=value`) to define a symbolic name for a numeric value. The symbolic name can be used on its own or associated with a numeric default value that is used if the symbolic has not been defined. The default value is specified as `name|value` as shown in the following examples:

```
SELECT NUMBERFIELD>HIGH
SELECT NUMBERFIELD>HIGH|20
```

In the CARLa command input, the symbolic name must be defined before its first use. If you use the conditional specification, the value is the default value that is used only if the SYMBOLIC statement has not been defined. For more information and usage restrictions, see “SYMBOLIC” on page 940.

Modifying the column header

If desired, a *column header* may be defined for the field. Generally the default header is sufficient, but if you use a non-default length, you may also want to use another header. This can be accomplished by specifying a string as modifier; the string must be enclosed in either single, double, or left quotations to distinguish it from an output format name. Possibly, you have to specify a different output length as well, because by default the header is truncated at the implied or specified field output length. The maximum length of the header string is 512 characters.

Changing the sort order

The LIST command produces output in order of processing; the SORTLIST, DISPLAY, and (D)SUMMARY commands produce sorted output. Output is sorted

column by column, from left to right, in ascending order. To compare subsequent output lines, all of the output fields are compared in turn, until a difference is detected. If a column contains a repeat group, only the first field of the unsorted repeat group is taken into account.

The following methods have been provided to change the sort order:

- The DESCENDING output modifier.
- The NONDISPLAY output modifier.
- The SORT output modifier.
- The SEARCHKEY and TREELINE fields in NEWLIST TYPE=RACF.

The DESCENDING output modifier changes the sort order for a column from ascending into descending. All other columns are still sorted in ascending order, and columns to the left are still compared before the current column. This means that using the DESCENDING output modifier in the third column from the left sorts all records in ascending order as determined by the first two columns; if the first two are equal, in descending order as determined by the third column; and if the first three are equal, in ascending order as determined by subsequent columns.

The NONDISPLAY output modifier can be used to 'hide' an output field. The column in which it is used is not displayed, and does not take up space on the screen or in a report. However, the content of the hidden column is still used to determine the sort order. The NONDISPLAY output modifier can therefore be used to specify a sort sequence different from the printed output. It is most often used to hide a first column containing the desired sort key , e.g. SEARCHKEY .

The SORT output modifier is used to sort repeat group entries within a column. It does not affect the overall sort order. See “Repeated field output modifiers: Changing display of Repeated fields” on page 804 for more information.

The SEARCHKEY and TREELINE are two fields that are provided especially to change the sort order. The SEARCHKEY field can be used to sort profile names in a 'natural' order: generic characters follow alphanumerical characters. The TREELINE field can be used to sort GROUP profiles in a sort order useful to create group-tree reports. To sort on either of these fields, use them as the first column, with the NONDISPLAY output modifier (neither field provides 'pretty' output).

Format names for input and output

When you generate commands in CARLa input and specify output options, you must ensure that input and output values have the proper syntax. zSecure provides format names to address this issue.

- “Specifying syntax for RACF command input”
- “Flag formats: Using available formats for flag field input and ouput” on page 826
- “Date output formats: Formatting date field output for different locales and standards” on page 828
- “Formatting UNIX file type, attribute, and audit flag fields” on page 823
- “COMPARE processing output formats: Formatting COMPARE_CHANGES results” on page 829

Specifying syntax for RACF command input: When you generate RACF commands in CARLa output, you must ensure that generated values have the proper syntax yourself. Many report formats have equivalents that start with a '$' character that are suitable for this.

$AsymKeyUsage
This formats the ASYMUSAGE(CSFAUSE) field as used in RACF commands RDEFINE and RALTER for the following general resource classes: CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY segment ICSF.

$CFSYN
Format to generate the FIRST and OTHER syntax specification for a RDEFINE and RALTER for general resource class CFIELD segment CFDEF. You must add the key, class, and segment parameters yourself.

$CUSTOM_DATA
Format to generate the CSDATA part of an ADDUSER, ALTUSER, ADDGRP, or ALTGRP command. The format prints the CSKEY followed by the CSVALUE in parentheses. You must add the key and segment parameters yourself. This format is only valid on the CUSTOM_DATA field.

$SymKeyExp
This formats the SYMEXPORTABLE (CSFSEXP) field as used in RACF commands RDEFINE and RALTER for the following general resource classes CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY segment ICSF.

ACCESS
Access level. The usual access levels are NONE, EXECUTE, READ, UPDATE, CONTROL and ALTER. For connects the access levels JOIN, CONNECT, CREATE and USE may be shown. For digital certificates this field may show the TRUST or NOTRUST status. In certain reports, or exploded/resolved/effective/trust access lists the special values OWNER, QUALOWN, CREATE, ALTER-M, ALTER-P, CKGOWNR, READLPA, LOADEXE, COPY, AUDIT and HIDDEN may occur. On an ACL field expanded with the EFFECTIVE or EXPLODE modifier ALTER-O may be shown.

ACLACCESS
Only valid for the ACL field or a subselect thereof. This format displays just the access level, optionally followed by a condition in parentheses: READ or READ(PROGRAM=CKRCARLA). It is meant for use with a define subselect ACL variable that selects a specific ID, * for example.

ACLID
Only valid for the ACL field or a subselect of this field. For each ACL entry, this format displays an ID in the output, optionally followed by a condition in parentheses. If the ACL is in normal format, the ID is the value of ACL id. If the ACL uses field modifiers like EXPLODE or EFFECTIVE, the ID is the value of the resolved user ID. The ACLID format is designed to format the output for a DEFINE SUBSELECT ACL variable that selects a specific access level. See also "ACLVIA."

ACLIDACCESS
Only valid for the ACL field or a subselect of this field. This format displays the ID followed by the access level and optionally a condition in parentheses. It is meant to display an access list in horizontal wrapped format.

ACLVIA
Only valid for the ACL field or a subselect of this field. This format generates output that is like the default ACL format, except that the first two columns of data, User and Access, are omitted. In other words, only the ACL ID and an optional condition (When) are shown. See also "ACLID."

ACSI
Filemode access intent. Formats a flag field in a 4-character field corresponding

with the UNIX_ACCESS_INTENT field, for example,*drwx*. See "UNIX_ACCESS_INTENT" on page 1375.

ADDRESS
Formats both 31-bit and 64-bit addresses. 31-bit addresses are printed as 8 hexadecimal characters, 64-bit addresses are printed as two blocks of 8 hexadecimal characters, separated by an underscore.

AFC
Audit function code. Formats a USS Audit function code in a 16-character field corresponding with the UNIX_FUNCTION field documented in "SMF: SMF records" on page 1276. A sample value of the field is 'unquiesce_setuid'. If the meaning of some function code *nnn* is (yet) unknown, it will be formatted as `AFC_nnn`.

ASIS
The field is copied without modification. The difference with CHAR is that trailing blanks are preserved. Note that with XML output, trailing blanks (as well as trailing null characters) are trimmed off anyway.

AUDAC, AUDLVL
Audit access level, for example the access level at which auditing starts. Can be blank, READ, UPDATE, CONTROL or ALTER.

AUDIT
Audit type, for example indication which accesses are logged. Can be ALL, SUCCESS, FAILURE, or NONE.

AUTHORITY
Connect authority. Can be USE, CREATE, CONNECT, or JOIN.

BLANK$HDR
Blank or header. Format a flag field as blanks if true or missing and as the header otherwise. An overriding length and header are generally required. See also HDR$BLANK.

BLANK$NO
Blank or no. Format a flag field as blanks if true or missing and as "No" otherwise.

BLANK$STR(*'string'***)**
Blank or string. Format a flag field as blanks if true or missing and as the specified string otherwise. An overriding length and header are generally required. The string can be enclosed in single, double, or left quotation marks. See also STR$BLANK.

CATEGORY
Security category in words. This format is invalid in a LIST statement. If the word value is unavailable, it displays the internal decimal value as <*nn*>. Maximum output length: 37 characters.

CHAR
Character string. The field is copied without modification, except that trailing blanks are not preserved. See also ASIS.

CHR$NOFF
This format is designed to handle character fields that are defined with a default value of x'FF'. This means a blank field is printed if every byte of the field contains x'FF', in any other case, the field is printed as is.

CMDAUTH
This formats a console command authorization in a 6-character field. It can be MASTER, ALL, INFO, or a combination of the letters C I S for CONS, IO, and SYS respectively.

CONNECTID
Only valid for the connects field or a subselect thereof. Prints a connect id from a subselect connects variable or a connects field as "id". It is meant for use with modifiers horizontal, word wrap.

CONTENTS, STRINGS
Print binary data in a condensed human-readable format. A sequence of consecutive printable characters is considered a text string when it has at least three characters or if it occurs at the end of the data. Text strings are printed. Data not part of a text string is condensed. A residual sequence of two or more characters is replaced by two dots. A residual single unprintable character is replaced by a single dot. See also PRINTABLE.

CONVSEC
Conversation security. Can be NONE, CONV, AVPV, PERSISTV, or ALREADYV.

CSVALUE
Value of a custom field. This setting formats the value of the custom field depending on its type. This format is only valid on the CUSTOM_DATA field.

DATE
Date is displayed in various formats. The basic layout is 11 characters long DD MMM YYYY (" 1 Jan 1997"). The layout is determined by the output length specified, as shown in the next section.

DATETIME
This formats a TIME BIN time stamp (CCYYDDDF + 4 byte centiseconds) as DD MMM YYYY HH:MM:SS.CC (12 Jan 1980 12:23:34.89)

DATETIMEZONE
This formats a TIME BIN time stamp (CCYYDDDF + 4 byte centiseconds) as YYYY-MM-DD,HH:MM:SS.D, *sign* HH:MM (e.g., 2003-1-26,13:30:15.0,-4:0). Since the time zone is not present in the input, it is taken from the system the input is associated with. For a DEFTYPE NEWLIST this requires a DEFINE for the field SYSTEM, which is interpreted as an SMF ID which is matched against the available CKFREEZEs (preferably in the same complex if the DEFTYPE allocation specified one). If the lookup fails, the time zone is taken from the default system (see “DEFAULT SYSTEM” on page 750). On a SUMMARY or for a BUNDLEBY variable the time zone is omitted. If the input length is not 8, the automatic time zone is disabled.

If the input field has a 12-byte value, the additional 4 bytes are interpreted as the high half of a TOD stamp. The parser might still issue CKR1228 or CKR1229 in advance to warn you when the automatic lookup is not supported. Add the CARLa command SUPPRESS MSG=(1228,1229) before your query to get rid of the warnings.

The intent of the output format is to be compliant with RFC 2579.

DATE$STR (*'string'***)**
Date or string. This format allows the user to specify a string to be returned when a date field has no value. The string can be enclosed in single, double, or left quotation marks. A valid date is displayed according to the basic date format. See also `DATE`.

DEC
DECIMAL
Decimal. This format accepts a 1, 2, 3 or 4-byte source integer. If it is a 4-byte integer and contains high-value bits only (X'FFFFFFFF), this is interpreted as *undefined* and nothing is printed. However, a 1-byte source value of 255 is printed as 255. If a 4-byte value is defined but has its most significant bit on, this is considered an error. If the number to be printed does not fit in the specified or implied column width, asterisks are printed (*). Note that a 1-byte value can always be printed in 3 positions, 2-byte in 5, 3-byte in 8, and 4-byte in 11. See also NUM.

DEC$ABBREVIATE
DEC$ABBR
This functions as the DEC format, but will abbreviate the number to fit into the specified or implied column width. It does so by dividing the number by powers of 10 (rounding normally), and inserting the appropriate SI multiplication factor (k, M, G, T, P, or E). For example, the number 10485760 is printed in a 4-character column as 10M5 and in a 6-character column as 10486k. Note that a minimum column width of 42-characters is needed for this format to work correctly. The value *0* is not printed, but blanks will be shown instead.

The format accepts source integers of up to 8 bytes. If the source integer has 4 or 8 bytes and it contains high-value bits only (X'FFFFFFFF' or X'FFFFFFFFFFFFFFFF'), this is interpreted as undefined and nothing is printed. Other 4-byte and 8-byte integers with a most significant bit of 1 are considered to be errors. Source integers with a length other than 4 or 8 are always interpreted as nonnegative integers. They are neither interpreted as undefined, nor considered to be errors.

DEC$BLANK DB
Decimal or blank. This functions like DEC, but displays blanks if the value is 0.

DEC$NO
This functions as the DEC format, but displays 'No' if the value is 0.

DOM
Delete Operator Message format. Can be blank, NORMAL, ALL, or NONE.

DSTYP
DSTYPE
Data set type. Can be blank, NONVSAM, GENERIC, VSAM, MODEL, TAPE or "n/a". Use this format to display the DSTYPE field from DATASET profiles.

DUMP
DUMP(*n*)
Dump format: *oooo. xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx *ccccccccccccccc** (offset in hexadecimal, contents in hexadecimal per fullword, contents as text with dots for nonprintables.). By default, the offset is shown as 4 hexadecimals; this number can be varied by specifying DUMP(*n*) for n hexadecimals. If n is 0, the separating dot and blank are suppressed. The dump format always displays an integer number of fullwords per line. With a default offset display, it requires a minimum effective output length of 21 (for 1 fullword), and 13 more positions per additional fullword; if the output length is smaller than the minimum length required to print one fullword, one asterisk(*) is printed. The default output length allows four fullwords to be printed (this number is 60 for a default offset display). This length is also selected if 0 is specified or implied. The WRAP (and WORDWRAP) modifiers are automatically implied and have no further effect; the HORIZONTAL modifier is flagged as an error.

EUDATE
This formats a date in European format. It returns the 10-character value 'DD-MM-YYYY'. If not enough space is available only the last 2 digits of the year will be shown. It is possible to override the separator to a / or a blank as follows: EUDATE('/') or EUDATE(' ').

EXTATTR
UNIX file extended attributes, e.g., 'apsl'. See "Formatting UNIX file type, attribute, and audit flag fields" on page 823.

FILEAUDIT
UNIX file audit flags. This parameter formats one set of audit flags (user, auditor, effective) for a UNIX file. as e.g. 'sfa' (*read successes*, *write failures*, *all executions*). See "Formatting UNIX file type, attribute, and audit flag fields" on page 823.

FILEMODE
UNIX file access flags. This parameter formats the access values *read*, *write* and *execute* for the owner, group, or other ID, rwxr-x--- for example. See "Formatting UNIX file type, attribute, and audit flag fields" on page 823.

FILETYPE
UNIX file type. '-' (regular file), 'b' (block special file), 'c' (character special file), 'd' (directory), 'e' (external link), 'l' (symbolic link), 'p' (pipe), 's' (socket). See "Formatting UNIX file type, attribute, and audit flag fields" on page 823.

FLAG
Format a flag field as "YES" if true, as blanks if false or missing and as '???' if unintelligible.

FLAG2NICE
This flag format displays true as "Yes", false as "No", missing as blanks and errors as '?'. FLDLEN This displays the length of the field as it is stored in the database (except for special keywords, where it generally returns the length of the external representation). If the field length to be printed does not fit in the output column width asterisks (*) are printed.

GID
Unix group id. Formats a UNIX group id as a signed decimal number, possibly followed by one of the associated RACF groupids between brackets. The decimal number can also be followed by '(undef)'. A sample value is '9000 (AGROUP)'.

HDR$BLANK
HB
Header or blank. Format a flag field as the header if true and as blanks otherwise. An overriding length and header are generally required. See also BLANK$HDR.

HEX
Hexadecimal. As a hexadecimal display requires twice as many output positions as the length of the input, an overriding length is generally required. Length 0 is recognized as 'natural length' (for example, twice the field length), but does not work with DISPLAY. If WRAP is also specified, output behavior with respect to output length follows the WRAP rules rather. If HEX,WRAP,0 is specified, the actual output length is rounded down to a byte boundary (even number), except for length 1. See also DUMP.

IP

This format takes either a 4 byte IPv4 address or a 16 byte IPv6 address and prints it as follows. A four byte address is printed as four decimal numbers separated by periods, `10.0.2.255` for example. For a 16 byte address each 2 byte block is printed in hex, dropping leading zeroes, separated by colons, `FE80:0:0:0:200:F8FF:FE01:9742` for example. This is compressed by removing the longest string of 2byte zero blocks as follows: `FE80::200:F8FF:FE01:9742`. Compressed addresses that do not fit the destination length will print the longest possible suffix (in 2 byte blocks) preceded by an asterisk, `*F8FF:FE01:9742` for example.

IPSQ
Formats IP addresses in the standard IP address format except that IPv6 addresses are enclosed in square brackets, `[ABCD::9876]` for example. The brackets are added to avoid confusion when an IPv6 address specification is followed by a colon and a port number, `ABCD::9876:1234` for example. When the brackets are added, it is easier to distinguish the port number from the IP address: `[ABCD::9876]:1234`.

IPV4OR6
This formats IP addresses in the standard IP address format, except that addresses of the form `::FFFF:a.b.c.d` are printed like `a.b.c.d`. This format can be useful in a context where `::FFFF:a.b.c.d` denotes a true IPv4 address rather than an IPv4-mapped IPv6 address.

IPV4OR6SQ
This formats IP addresses in the same way as the `IPSQ` format does, except addresses of the form `::FFFF:a.b.c.d` are printed like `a.b.c.d`, without enclosing square brackets. This format can be useful in a context where `::FFFF:a.b.c.d` denotes a true IPv4 address rather than an IPv4-mapped IPv6 address.

JULDATE
JULIANDATE
This formats a date in Julian format, `YYYY/DDD` for example.

KEYUSAGE_RACF
This formats the CERTIFICATE_KEYUSAGE field as RACF interprets it. When combined with the EXPLODE modifier it shows the following values as separate entries in a repeated field: HANDSHAKE, DOCSIGN, DATAENCRYPT and CERTSIGN. When used without EXPLODE it will represent each of these values with a single character (e.g., 'HDEC').

KEYUSAGE_X509
This formats the CERTIFICATE_KEYUSAGE field as defined by the X.509 standard. When combined with the EXPLODE modifier it shows the following values as separate entries in a repeated field: `digitalSignature`, `nonRepudiation`, `keyEncipherment`, `dataEncipherment`, `keyAgreement`, `keyCertSign`, `cRLSign`, and `encipherOnly`. When used without EXPLODE, this setting represents each of these values with the two characters, `dSnRkEdEkAkCcSeO` for example.

L1ASIS
This format copies input strings to the output prefixed by a length byte. Trailing blanks are preserved. This format can be used to create file output. For example, in zSecure Admin, this format is used to create the output file in the Access Monitor consolidation process. L1ASIS is usually used with overriding length 0. Also, see the L1CHAR format name.

The formats L1CHAR and L1ASIS sort on field length before sorting on the character content of the field.

L1CHAR
This format performs the same function as L1ASIS, except that trailing blanks are not preserved.

The formats L1CHAR and L1ASIS sort on field length before sorting on the character content of the field.

LOGDAYS
This formats a byte according to the setting for `logon-allowed` days, in the form SMTWTFS, where the day-of-week letter indicates that logon is *permitted*, and is left blank otherwise. This format can also be used with the EXPLODEoutput modifier and an overriding length of 3; in that case, the first seven bits in the byte are each exploded to 'YES' if set or 'NO' if not set.

LOGTIME
This formats a `logon-allowed` time frame as HHMM:HHMM, blanks, or ANYTIME.

LOWERCASE
Format a string into all-lowercase characters, e.g. '*Ad Grant*' is formatted as '*ad grant*'. Strings longer than 256 bytes are truncated.

MFORM
This formats a message format in a 5-character field. It can be a combination of the letters TSJMX for displaying time stamp, originating system, job ID/name, message text, and excluding exempt messages, respectively.

MONITOR
This formats a message monitor status in a 5-character field. It can be a combination of the letters JtStF. 'J ' and 'Jt' are displayed for JOBNAMES and JOBNAMEST respectively, 'S ' and 'St' for SESS and SESST, respectively. 'F' is displayed for STATUS.

MONTH
The month as a text string: 'January' to 'December'.

MONTHDAY
This formats the day of the month in a date as two digits where the first might be blank as in ' 1' to '31'.

MSGLEVL
This formats a console message level from the RACF field OPERLEVL in the OPERPARM segmentin a 14 character field. The first 12 characters can be ALL or a combination of the letters R I CE E IN. The last two characters are NB or blank. The meaning of the letters is:

NB
No broadcast messages

ALL
Same as R I CE E IN

R Messages requiring an operator reply

I Immediate action messages

CE
Critical Eventual action messages

E Eventual action messages

IN
Informational messages

MVSMSGLEVEL
This formats a console message level from the z/OS EMCS console definitions in a 14 character field. The first 12 characters can be ALL or a combination of

the letters R I CE E IN. The last two characters are NB or blank. The meaning of the letters can be found in the description of the MSGLEVL format.

NOSORTLIST
This modifier can be used to prevent this column to be part of the record sort key as defined by the SORTLIST or SUMMARY command. It is however more efficient CPU wise to use "field(nondispl)" in front of the visible fields to identify sort keys. On the other hand, it makes for convenient and less complex CARLa coding.

NUM
This formats a 1, 2, 3, or 4-byte binary integer as a decimal number with a field name-dependent length. The length can be overridden. If the value contains a high-value (all bits on), blanks are displayed (this is the RACF database value for 'undefined') . To format high-values as a number, use the DEC format.

OCTAL
UNIX file access flags in octal notation, e.g. 0750. See “Formatting UNIX file type, attribute, and audit flag fields” on page 823.

OPERUND
OPERparm
Receive undeliverable messages format (UND). This flag format displays true as "YES", false as "NO", missing as blank and errors as "?". As an input format it is specially suited for the OPERUD template field - see “Flag formats: Using available formats for flag field input and ouput” on page 826.

PGMRNAME
Print the field in character format. This format is specially designed for the `pgmrname` field in the RACF user profiles. If the field contains the RACF default value for the `pgmrname` (20 # symbols), the value is output as blank characters.

PORT
Format a numeric IP port textually. The port descriptions are taken from the Internet Assigned Numbers Authority (IANA). See http://www.iana.org/assignments/port-numbers. You can use this format with DSTPORT and SRCPORT in SMF NEWLIST.

PRINTABLE
Print binary data in a human-readable format. Each unprintable character is replaced by a dot. See also CONTENTS.

RACFLEVEL
This format is meant for use with the RCVT_RACFLEVEL field. It takes a RACF software level like '2060' or '7705' as input, and formats it with dots, like '2.6.0' or '7.7.5'.

RESFLG
This displays the RESFLG flag field of a general resource profile in a 3 character field, in the form SAT. The character S indicates a TAPEVOL that might contain only one data set (singledsn); the character A indicates an automatic TAPEVOL; the character T indicates a TVTOC is maintained. A blank indicates the option is not set. This format can also be used with the EXPLODE output modifier and an overriding length of 11, e.g. RESFLG(EXPLODE,11). When exploded, the options are displayed in full, for example AUTOMATIC/NOAUTOMATIC, SINGLEDSN/NOSINGLEDSN, and TVTOC/NOTVTOC.

ROUTCDE
This formats a routing code bitstring as a list of routing codes ranges, separated by commas.

SECLEVEL
Security level in words. This format is invalid in a LIST statement. If the word value is unavailable, it displays the internal decimal value as <*nn*>. Maximum output length: 38 characters.

SECURPASS_DATE
This formats the date field, as found in SECURPASS SMF records.

SECURPASS_RC
This prints the return code as found in a SECURPASS SMF record as a human readable string, explaining the result.

SECURPASS_REQUEST
This prints the request code as found in a SECURPASS SMF record as a human readable string, explaining type of request.

SIGNEDDEC
Signed Decimal. This format accepts a 1, 2, 3, or 4-byte signed integer and prints it decimally, optionally preceded by a minus sign. If the value to be printed does not fit in the specified output length, asterisks are printed instead.

SLKEY_COMPACT
This format is only valid on the CICS_RSLKEY and CICS_TSLKEY pseudofields in NEWLIST type RACF. Instead of printing each Security Level Key individually, as is done normally for those fields, it combines them into continuous ranges. For example a list of keys like '12 13 14 15 23 35 36 37' will be printed as '12:15 23 35:37'.

SMFTIME
Format a binary 4-byte time value in 1/100s (e.g., from an SMF record) as a time. The maximum output length of this field is 11 characters (formatted 'HH:MM:SS.CC'), other output lengths are 8 ('HH:MM:SS'), 5 ('HH:MM') and 4 ('HHMM', valid for CARLa select statement input). Other lengths revert to the largest of these that can be accommodated, blank-padded, with the exception of length 10 which uses the longest format but truncates; lengths smaller than 4 use 'HH:MM' but truncate.

SMFTIMESTAMP
This formats an SMF time stamp, containing both date and time as DD MMM YYYY HH:MM:SS.CC (12 Jan 1980 12:23:34.89)

SMFTIMESTAMPZONE
This formats an SMF time stamp (4 byte centiseconds + CCYYDDDF) as YYYY-MM-DD,HH:MM:SS.D,*sign*HH:MM (e.g., 2003-1-26,13:30:15.0,-4:0). Since the time zone is not present in the input, it is taken from the system the input is associated with. For a DEFTYPE NEWLIST this requires a DEFINE for the field SYSTEM, which is interpreted as an SMF ID which is matched against the available CKFREEZEs (preferably in the same complex if the DEFTYPE allocation specified one). If the lookup fails, the time zone is taken from the default system (see “DEFAULT SYSTEM” on page 750). On a SUMMARY or for a BUNDLEBY variable the time zone is omitted. If the input length is not 8, the automatic time zone is disabled.

If the input field has a 12-byte value, the additional 4 bytes are interpreted as the high half of a TOD stamp. The parser might still issue CKR1228 or CKR1229 in advance to warn you when the automatic lookup is not supported. Add the CARLa command SUPPRESS MSG=(1228,1229) before your query to get rid of the warnings. STR$BLANK

STR$BLANK(*'string'***)**
String or blank. Format a flag field as the specified string if true and as blanks

otherwise. An overriding length and header are generally required. The string can be enclosed in single, double, or left quotation marks. See also BLANK$STR.

TIME
Format an unsigned packed decimal 4-byte time value in 1/100s (e.g., from a RACF profile) as a time. The maximum output length of this field is 11 characters (formatted 'HH:MM:SS.CC'), other output lengths are 8 ('HH:MM:SS'), 5 ('HH:MM') and 4 ('HHMM', valid for CARLa select statement input). Other lengths revert to the largest of these that can be accommodated, blank-padded, with the exception of length 10 which uses the longest format but truncates; lengths smaller than 4 use 'HH:MM' but truncate.

TOD
This formats a TOD time stamp as DD MMM YYY HH:MM:SS.uuuuuu (12 Jan 1980 12:23:34.897654)

TSOOPT
This formats TSO logon options in a 4-character field. It can be a combination of the letters MNRO for MAIL, NOTICE, RECOVER and OIDCARD, respectively.

UDEC
This format takes a hexadecimal number of up to 8 bytes in length and prints it as an unsigned decimal number.

UDEC$ABBREVIATE
UDEC$ABBR
This format takes an unsigned integer of up to 8 bytes in length and prints it as an unsigned decimal number. The value is abbreviated to fit into the specified or implied column width based on the following calculation: The number is divided by powers of ten (rounding normally), and the appropriate SI multiplication factor is inserted (`k`, `M`, `G`, `T`, `P`, `E`, or `Z`). For example, the number 10485760 is printed in a four-character column as *`10M5`*. In a six-character column, the value is printed as `10486k`.

This format requires a column that is at least 2-characters wide to work correctly.

UID
UNIX user ID. Formats a UNIX user ID as a signed decimal number, possibly followed by one of the associated RACF user IDs between brackets. The decimal number also might be followed by `(undef)`. A sample value is `10002 (SOMEUSER)`.

UPPERCASE
Format a string into all-uppercase characters, e.g. 'Ad Grant' is formatted as 'AD GRANT'. Strings longer than 256 bytes are truncated.

UPT
This formats a TSO user profile table in a 15 character field. It consists of the user prefix (7 characters), a blank, and a combination of the letters PI?MOWR for PROMPT, INTERCOM, PAUSE, MSGID, MODE, WTPMSG, and RECOVER, respectively.

USDATE
This formats a date in US format. It returns the 8-character value 'MM/DD/YY' even if the year is beyond 2000, for use by applications that work this way.

USRDATA
Format to print only the USRDATA from the USR field.

WEEKDAY
The day of the week as a text string: 'Sunday' to 'Saturday'.

WHEN
This formats a condition in the template field ACL2RSVD in the form:*class profile*.

XSD_DATETIME
This format is intended to print XML-compliant time stamps according to ISO 8601. In an XML schema this is represented as "xsd:dateTime", or in the older (1999) specification "xsd:timeInstance". The format lists as YYYY-MM-DDTHH:MM:SS.CC+hh:mm where the time zone is left out if unknown. All numbers print with leading zeroes, for example, subfield offsets are fixed within this format.

YEAR
This formats the year of a date value in 4 digits.

YESNO
Yes or No (mixed case). This flag format displays true as "Yes", false and in error as "No", and missing as blanks. It can also be used with the EXPLODE output modifier; in that case, all 8 bits in a byte are exploded to the value "Yes" or "No".

$ACL
Format to generate the trailing part of a RACF PERMIT command that contains the ID, ACCESS, and WHEN parameters. You must add the profile key and CLASS parameter yourself. The format can only be applied to the field name ACL.

$AUDITLVL
Format to generate the AUDIT or GLOBALAUDIT parameters for an ALTDSD or RALTER command. It can only be applied successfully to the fields AUDITLVL and GAUDITLVL.

$CASE
This flag format displays true as "ASIS", false and in error as "UPPER", and missing as blanks. It can be used for formatting the CASE subparameter of the CDTINFO parameter of an RDEFINE or RALTER command.

$CHAUDIT
UNIX file audit flags command format for use with the**chaudit** command, e.g., 'r=s,w=f,x=sf' (read successes, write failures, all executions). See “Formatting UNIX file type, attribute, and audit flag fields” on page 823.

$CHMOD
UNIX file access flags command format for use with the **chmod** command, e.g., 'o=,u=rwx,g=rx' (user read/write/execute, group read/execute, other no access). See “Formatting UNIX file type, attribute, and audit flag fields” on page 823.

$CMDAUTH
Format to generate the string to be included between parentheses in the AUTH subparameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command. $CONDQT

$CONDQT
Format to print a field normally or in quotations depending on the contents. If the string contains a comma, semicolon, parenthesis, or blank, a quoted string is printed. If the string is printed in quotations, all occurrences of a quotation are doubled.

$CONNECT
Format to generate the trailing part of a RACF CONNECT command containing the AUTH, UACC, SPECIAL, OPER, AUDITOR, ADSP, GRPACC, REVOKE, REVOKEDT, and RESUMEDT parameters. You must add the user ID and GROUP parameter yourself. The format can only be applied to the field name CONNECT.

$DATE
Format to generate the ISO standard date format YYYY-MM-DD.

$DOM
Format to generate the string to be included between parentheses in the DOM sub-parameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command.

$EXTATTR
UNIX file extended attributes command format for use with the extattr command, for example, '+as,-pl' (APF authorized, share address space might be honored). See “Formatting UNIX file type, attribute, and audit flag fields” on page 823.

$LOGCMDR
Format to generate the string to be included between parentheses in the LOGCMDRESP sub-parameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command.

$LOGDAYS
Format to generate the content of the 'when(days())' parameter for generating an ALTUSER, ADDUSER, RALTER, or RDEFINE command.

$LOGTIME
Format to generate the content of the 'when(time())' parameter for generating an ALTUSER, ADDUSER, RALTER, or RDEFINE command.

$LOGZONE
This formats a 3 byte packed decimal RACF time zone (0HHMMS) as "W HH.MM"/"E HH.MM". This is intended for the creation of commands in the TERMINAL General Resource class, in the TIMEZONE field.

$MEMLST
Format to generate the string to be included between parentheses of the ADDMEM operand of the RDEF and RALTER command.

$MFORM
Format to generate the string to be included between parentheses in the MFORM sub-parameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command.

$MONITOR
Format to generate the string to be included between parentheses in the MONITOR sub-parameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command.

$MSGLEVL
Format to generate the string to be included between parentheses in the LEVEL sub-parameter of the OPERPARM parameter of an ADDUSER or ALTUSER RACF command.

$NO
Command generation for No. Format a flag field as blanks if true or missing and as "no" otherwise. It is meant for generating RACF command parameters

like SPECIAL/NOSPECIAL. This format can also be used with the EXPLODE output modifier; it gives identical results.

$QUOTED
Format to print a field while doubling all occurrences of a single quote. You must supply the leading and the trailing quotation yourself.

$RACLINK
Format to generate the DEFINE or APPROVE keywords and parameters for use in a RACLINK command. The $RACLINK format can only be used to format the RACLINK field of the USER profile, and does not include the user ID itself.

The full RACLINK command can be used to recreate a RACLINK association. In addition to the required keywords, the $RACLINK format can generate comments indicating the status of the RACLINK association at hand.

- `/* Unknown link type */` The link type is not PEER, MANAGER OF, or MANAGED BY,
- `/* Master */` The link type is MANAGED BY,
- `/* Reserved bit used */`
- `/* Rejected */`
- `/* Pending on local node */`
- `/* Pending on remote node */`

$RESFLG
Format to print the RESFLG field of a general resource profile for a RDEFINE or RALTER command.

$RETPD
This formats a two byte hexadecimal number as a RACF retention period. This intended for the creation of commands in the DATASET class, in theRETPDfield.

$SYN
This format displays the syntax rules of profiles as a list of text strings: "ALPHA", "NATIONAL", "NUMERIC", and, "SPECIAL". It can be used for formatting the FIRST and OTHER subparameters of the CDTINFO parameter of an RDEFINE or RALTER command.

$TIMEOUT
Format to print the TIMEOUT field of the CICS segment of a user profile for a RDEFINE or RALTER command.

$USRDATA
Format to print the USR field in a format suitable to generate a CKGRACF USRDATA command, for example *index(value)*.

$XRFSOFF
Format to generate the string to be included between parentheses in the XRFSOFF subparameter of the CICS parameter of an ADDUSER or ALTUSER RACF command.

$YESNO
Command generation Yes or No. This flag format displays true as 'YES', false and in error as "NO" and missing as blanks. It is meant for generating RACF command parameters like MIGID(NO). This format can also be used with the EXPLODEoutput modifier; in that case, all 8 bits in a byte are exploded to the value 'YES' or 'NO'.

Formatting UNIX file type, attribute, and audit flag fields: This section provides overviews of various output formats used with the UNIX file system.

Specifically, we look here at the formats for file type, attributes, extended attributes and audit flags.

When you issue the **ls** command from a standard OMVS shell with the **-laEW** options, you obtain a listing (somewhat) like the following:

```
total 40
drwx------+ fff---      2 C##BJT2  C##BOMVS    8192 Jan 25 13:33 .
dr-xr-xr-x  ------     38 R##SLIN  SYSAPPL        0 Jan 25 14:52 ..
-rwxr-----  fff--- --s  1 C##BJT2  C##BOMVS     749 Jan 25 13:48 .profile
-rw-------  fff--- --s  1 C##BJT2  C##BOMVS     286 Jan 25 16:42 .sh_history
```

The leftmost column shows the file type in the first position (TYPE), the file's attributes (ATTR), and whether the file has any (extended) ACL entries. The second column shows the audit flags (AUDITFLAGS_USER, AUDITFLAGS_AUDITOR). The third column shows the file's extended attributes (EXTATTR). The other columns show the number of hard links to the file (LINK_COUNT), the owner (OWNER), the group (GROUP), the file size, the last change date (for a file; for a directory the creation date), and the pathname. The field names shown in brackets refer to NEWLIST TYPE=UNIX.

There are three different types of ACLs that can be associated with a UNIX file: an access ACL (EXTENDED_ACL), a directory default ACL (DIRECTORY_DEFAULT_ACL) and a file default ACL (FILE_DEFAULT_ACL). The last position of the first column corresponds with the OR of these three, which can be defined as follows.

```
DEFINE TYPE=UNIX ANY_ACL TRUE WHERE EXTENDED_ACL OR,
                                DIRECTORY_DEFAULT_ACL OR FILE_DEFAULT_ACL
```

File type: The following table list the possible file type values (FILETYPE format).

TYPE	file type	meaning
-	regular file	contains data
b	block special file	e.g., a disk or CD-rom (but this does not occur in USS)
c	character special file	e.g., a tty or printer
d	directory	contains files
e	external link	is a UNIX name for an MVS data set, or a PDS(E) member
l	symbolic link	contains another UNIX pathname to look up instead
p	pipe (or FIFO)	is a FIFO communication stream between two programs
s	socket	is a network connection

Note that 'hard link' is not a file type. In UNIX a file does not really have a name but is identified by an inode number. A file is primarily referred to via one or more path names (known as *hard links*) where that `inode` number appears in the directory.

The preceding example listing shows two directories and two regular files.

File attributes: Standard access control to the file is provided via the OWNER and GROUP in combination with the attributes. The attributes form three groups, the first of which shows the access the OWNER has, the second the access the other members of the GROUP have, and the third the access anyone else has. Each group consists of three positions. The first position shows whether read access is permitted (r), the second whether write access is permitted(w), and the third whether execute access is permitted(x).

In the preceding example listing, the .profile file can be read, written and executed by C##BJT2, and read by the other members of group C##BOMVS; other access is not permitted. The parent (..) directory of the one listed in the example can be read and executed by anyone, but no one has write access to it.

Furthermore, the third positions in the three groups are used to show whether the file has the setuid property, the setgid property and/or the sticky bit property, respectively. The setuid and setgid property are shown as 's' (when combined with execute access, or as 'S' without it), the sticky bit is shown as 't' (when combined with execute access, or as 'T' without it).

If a file has the setuid or setgid property, this means that when it is executed, it does not run under the effective permissions of the user/process executing it, but changes to those of the OWNER or GROUP associated with the file, respectively.

For a regular file, the sticky bit causes on execution a search for the program in the user's STEPLIB, the link pack area, or link list concatenation. For a directory, the sticky bit allows files in a directory or subdirectories to be deleted or renamed only by the owner of the file, by the owner of the directory, or by a superuser.

If a file has an (extended) access ACL, there are additional users and groups that have access. The file owner takes precedence over user entries on the ACL, which are more important than any group entries. All group entries (owning group or ACL) are equal, and if any group gives you access, you have that access. The file default ACL is copied to files created in a directory, and likewise the directory default ACL becomes the access ACL of a subdirectory when it is created (both default ACLs are also copied as default ACLs to the subdirectory).

The default output format for the ATTR and PHYSICAL_ATTR fields, FILEMODE, formats the access control bits like **ls**. There are two other output formats suited for these fields, OCTAL and CHMOD.

OCTAL	Permission	FILEMODE	CHMOD
4000	Setuid	--S------	go=,u=s
2000	Setgid	-----S---	uo=,g=s
1000	Sticky bit	--------T	ug=,o=t
0400	Owner can read	r--------	go=,u=r
0200	Owner can write	-w-------	go=,u=w
0100	Owner can execute	--x------	go=,u=x
0040	Group can read	---r-----	uo=,g=r
0020	Group can write	----w----	uo=,g=w
0010	Group can execute	-----x---	uo=,g=x
0004	Other can read	------r--	ug=,o=r
0002	Other can write	-------w-	ug=,o=w

OCTAL	Permission	FILEMODE	CHMOD
0001	Other can execute	---------x	ug=,o=x

The CHMOD format, refers to the three groups (owner, group and other) of the FILEMODE mode format with the letters 'u' (user), 'g' (group) and 'o' (other). It lists for each group what permissions are set by enumerating them, for example u=rwxs (owner may read, write, and execute, and the setuid property applies). If more groups have the same attributes, it lists them once, for example go= (group and other have no access). It separates different access indications with commas. The output can be used in a **chmod** command to restore a file to those permissions.

Audit flags: The audit flags indicate the auditing requested by the user and auditor, in two groups of three positions (for the access types read, write and execute). Each position shows one of the indications '-' (no auditing), 'f' (failure auditing), 's' (success auditing) or 'a' (both failures and successes). The effective audit settings are the requests of the user and auditor combined.

The CHAUDIT format refers to the three access types as 'r' (read), 'w' (write), and 'x' (execute). It lists for each what attempts are audited, by enumerating them, e.g., r=sf (for read access both successes and failures are audited). If more access types have the same audit settings, it lists them once, e.g., wx=f (for write and execute access only failures are audited). It separates different access indications with commas. The output can be used in a **chaudit** command to restore a file to those audit settings (for either user or auditor); if the settings are for the auditor settings, the **-a** option of the command should be used.

In the preceding example listing, both regular files show that the user requests failure auditing for all types of access, and there is no auditor requested auditing.

Extended attributes: The extended attributes are indicated by 'a', 'p', 's' and when on, and '-' when off. These abbreviations stand for APF authorization, Program control, Sharing of the address space setting honored (_BPX_SHAREAS), and Library sharing.

The $EXTATTR format lists the extended attributes by enumerating them, e.g., +ap, -sl (APF authorized, program controlled, does not honor _BPX_SHAREAS and does not use Library sharing). The output can be used in an **extattr** command to restore a file to those extended attributes.

Flag formats: Using available formats for flag field input and ouput: For your convenience this section includes some overviews of the varying flag formats. In addition the concept of *input* and *output* formats is explained here.

When a flag field is read by the program, its value is translated to one of the logical values **true**, **false**, **missing** or **in error**. This translation generally varies with the (database) field; an internal knowledge base takes care of this. As a user you only need to specify how each logical value is displayed by specifying the desired output format.

The following table lists how the various output formats print these logical values.

Table 297. Flag output formats

Output format	TRUE	FALSE	MISSING	ERROR (or value 3)
BLANK$HDR	blank	header	blank	= FALSE
BLANK$NO	blank	"No"	blank	= FALSE
BLANK$STR	blank	string	blank	= FALSE
FLAG	"YES"	blank	blank	"???"
FLAG2NICE	"Yes"	"No"	blank	"?"
HDR$BLANK	header	blank	blank	= FALSE
OPERUND	"YES"	"NO"	blank	"?"
STR$BLANK	string	blank	blank	= FALSE
YESNO	"Yes"	"No"	blank	= FALSE
$CASE	"ASIS"	"UPPER"	blank	= FALSE
$DOM	"NORMAL"	"ALL"	blank	"NONE"
$LOGCMDR	"SYSTEM"	"NO"	blank	= FALSE
$NO	blank	"no"	blank	= FALSE
$XRFSOFS	"FORCE"	"NOFORCE"	blank	= FALSE
$YESNO	"YES"	"NO"	blank	= FALSE

Occasionally you might want to display a flag field that the program does not recognize as such. For example, an SMF_FIELD that you defined. When that happens the program uses an input format (translation of input values to logical values) depending on the specified output format. (At this time it is not supported to change the input format independently of the output format).

The following table lists what input values are interpreted as what logical values in this case.

Table 298. Logical values as translated from input values if the input is not a flag field, depending on the effective output format

Output format	TRUE	FALSE	MISSING	ERROR (or value 3)
BLANK$HDR	first byte x'80'	first byte not x'80	input length 0	-
BLANK$NO	first byte x'80' or x'01'	first byte not (x'80 or x'01')	input length 0	-
BLANK$STR	first byte x'80'	first byte not x'80'	input length 0	-
FLAG	first byte x'80' or x'01'	first byte x'00' or x'40'	input length 0, or first byte x'FF'	first byte anything else
FLAG2NICE	first byte x'80'	first byte x'40'	input length 0, or first byte x'00'	first byte anything else
HDR$BLANK	first byte x'80'	first byte not x'80	input length 0	-

Table 298. Logical values as translated from input values if the input is not a flag field, depending on the effective output format (continued)

Output format	TRUE	FALSE	MISSING	ERROR (or value 3)
OPERUND	first byte x'80'	first byte x'40'	input length 0, or first byte x'00' or x'10'	first byte anything else
STR$BLANK	first byte x'80'	first byte not x'80'	input length 0	-
YESNO	first byte x'80'	first byte not x'80'	input length 0	-
$CASE	first byte x'80'	first byte not x'80'	input length 0	-
$DOM	first byte x'80'	first byte x'40'	input length 0, or first byte anything else	first byte x'20'
$LOGCMDR	first byte x'80'	first byte not x'80'	input length 0	-
$NO	first byte x'80' or x'01'	first byte not (x'80' or x'01')	input length 0	-
$XRFSOFS	first byte x'80'	first byte not x'80'	input length 0	-
$YESNO	first byte x'80' or x'01'	first byte not (x'80' or x'01')	input length 0	-

Note that x'80' is always seen as **true**, x'40' is always seen as **false**, and a field that is not present is always **missing**, so if this is appropriate, there is nothing to worry about. Further note that FLAG sees x'FF' as an 'undefined' value (as is usual in e.g. the RACF database).

Date output formats: Formatting date field output for different locales and standards: zSecure provides an extensive set of DATE format types to output the date information in displays and reports. These format types include: Julian, US, and European. Dates can also be output in TOD (Time-of-Day) format. Each format type also provides different length and display options. For examples, see Figure 514 on page 829

The following figure lists the various DATE formats. Three example dates are used.

length	date	usdate	juldate	$date	eudate
12	1 Mar 2002	03/01/02	2002/060	2002-03-01	01-03-2002
11	1 Mar 2002	03/01/02	2002/060	2002-03-01	01-03-2002
10	01Mar2002	03/01/02	2002/060	2002-03-01	01-03-2002
9	01Mar2002	03/01/02	2002/060	2002-03-0	01-03-02
8	1Mar02	03/01/02	2002/060	2002-03-	01-03-02
7	1Mar02	03/01/0	02.060	2002-03	01-03-0
6	1 Mar	03/01/	02.060	2002-0	01-03-
5	1Mar	03/01	02060	2002-	01-03
4	1	03/0	060	2002	01-0
3	1	03/	060	200	01-
2	1	03		20	01
1		0		2	0

length	date	usdate	juldate	$date	eudate
12	31 Dec 1997	12/31/97	1997/365	1997-12-31	31-12-1997
11	31 Dec 1997	12/31/97	1997/365	1997-12-31	31-12-1997
10	31Dec1997	12/31/97	1997/365	1997-12-31	31-12-1997
9	31Dec1997	12/31/97	1997/365	1997-12-3	31-12-97
8	31Dec97	12/31/97	1997/365	1997-12-	31-12-97
7	31Dec97	12/31/9	97.365	1997-12	31-12-9
6	31Dec	12/31/	97.365	1997-1	31-12-
5	31Dec	12/31	97365	1997-	31-12
4	31	12/3	365	1997	31-1
3	31	12/	365	199	31-
2	31	12		19	31
1	3	1		1	3

Figure 514. Date format examples for US, Julian, and European format types

length	tod	datetime
27	12 Mar 2005 01:59:59.522816	23 Apr 2009 09:46:38.39
26	12 Mar 2005 01:59:59.52281	23 Apr 2009 09:46:38.39
25	12May2005 01:59:59.522816	23Apr2009 09:46:38.39
24	12 Mar 2005 01:59:59.522	23 Apr 2009 09:46:38.39
23	12May2005 01:59:59.5228	23Apr2009 09:46:38.39
22	12May05 01:59:59.52281	23Apr09 09:46:38.39
21	12May2005 01:59:59.52	23Apr2009 09:46:38.39
20	12 Mar 2005 01:59:59	23 Apr 2009 09:46:38
19	12May05 01:59:59.52	23Apr09 09:46:38.39
18	12May2005 01:59:59	23Apr2009 09:46:38
17	12May05 01:59:59	23Apr09 09:46:38
16	12May05 01:59:59	23Apr09 09:46:38
15	12May2005 01:59	23Apr2009 09:46
14	12May05 01:59	23Apr09 09:46
13	12May05 01:59	23Apr09 09:46
12	12 Mar 2005	23 Apr 2009
11	12 Mar 2005	23 Apr 2009
10	12May2005	23Apr2009
9	12May2005	23Apr2009
8	12May05	23Apr09
7	12May05	23Apr09
6	12 May	23 Apr
5	12May	23Apr
4	?	?
3	?	?
2	?	?
1	?	?

Figure 515. TOD Date Format example

COMPARE processing output formats: Formatting COMPARE_CHANGES results: Use the following output formats for reporting compare processing results from the COMPARE_CHANGES option. (See "Defining variables for comparison results (COMPAREOPT)" on page 754.)

CMPCHG

This format is a flat condensed output format intended for a value defined as COMPARE_CHANGES. This format is defined as *field*(*value -> value*).

The value between parenthesis is either a value pair with an > symbol in between, or if the field is a repeated field, the values are enclosed between curly brackets: *field*({*value -> value*}). The curly brackets are included if a repeat group has more than one different value. If a value is missing, it is absent in this display format as shown in the following example.

```
CGGRPNM({>{H})
```

The output format CMPCHG can be combined with the HORIZONTAL modifier. The horizontal modifier is applied after the CMPCHG format. The following examples show examples of output with and without the modifier.

Without the horizontal modifier:

```
DFLTGRP(A->C)
CGGRPNM({A,B}->{C,E,F})
```

With the horizontal modifier:

```
DFLTGRP(A->C) CGGRPNM({A,B}->{G,E,F})
```

CMPCHG3

This format for DEFINE COMPARE_CHANGES is like the CMPCHG4 format but without the compliance direction column that indicates whether the change increases or decreases security. The CMPCHG4 format contains the changes detected during the comparison process. This format lists only the fields that have changed, not all comparison fields. The difference found is shown in the form of quadruplets (field name, compliance direction, baseline value, changed value). If the field name is that of a repeated field, the name is repeated as often as necessary to list the differences. In this situation, the baseline value and the changed value shown on any single line need not be related in any way. Instead, the repeat group entries are presented in an alphabetic sequence as shown in the following example.

```
Fieldname       Value-1                         Value-2
CGGRPNM         A                               G
CGGRPNM         B                               E
CGGRPNM                                         F
DFLTGRP         A                               C
```

The COMPARE_CHANGES field is sorted on the Fieldname, which is character format. If the field names are the same, the COMPARE_CHANGES field is sorted on the formatted value of Value-1.

You cannot change the sort order using either the SORT or DESCENDING format modifiers.

CMPCHG4

Default format for the DEFINE COMPARE_CHANGES specification.

This format contains the changes detected during the comparison process. This format lists only the fields that have changed, not all comparison fields. The difference found are shown in the form of quadruplets (field name, compliance direction, baseline value, changed value). If the field name is that of a repeated field, the fieldname is repeated as often as necessary to list the differences. In this situation, the baseline value and the changed value shown on any single line need not be related in any way. Instead the repeat group entries are presented in an alphabetic sequence, as shown in the following example:

```
Fieldname             C Value-1                 Value-2
CGGRPNM                  A                       G
CGGRPNM                  B                       E
CGGRPNM                                          F
DFLTGRP                  A                       F
```

The COMPARE_CHANGES field is sorted on the Fieldname, which is in character format. If the field names are the same, the COMPARE_CHANGES field is sorted on the formatted value of Value-1, and so on.

The sort order cannot be changed by the SORT or DESCENDING format modifiers.

CMPBASV
This overriding output format is intended for a value defined as COMPARE_CHANGES. The output format shows the baseline value of the field. This format can be used as a method to display the third column only of the CMPCHG4 format.

CMPCHGC
This format is much like CMPCHG but adds an extra plus sign (+) or minus sign (–) behind it to indicate whether the change resulted in an increase or decrease in security compliance.

CMPCHGD
This overriding output format is intended for a value defined as COMPARE_CHANGES. It shows the compliance change of the field. Another way to use this output format is as a method to display the second column of the CMPCHG4 format. Possible values for this format include a plus sign (+) or a minus (-) sign.

CMPCHGV
This overriding output format is intended for a value defined as COMPARE_CHANGES. It shows the changed value of the field. Another way to use this output format is as a method to display the fourth column of the CMPCHG4 format.

CMPFLD
This overriding output format is intended for a value defined as COMPARE_CHANGES. Specifying this format results in reporting only field names where a difference was found. The difference between this format and the CMPFLDN format is that the latter repeats the same field name if needed for listing the values in a format similar to CMPCHG4.

CMPFLDC
This overriding output format is intended for a value defined as COMPARE_CHANGES. It results in reporting the field names where a difference was found. This format is like the CMPFLD format. However, it adds an optional compliance direction (+/-) after the reported field names to indicate whether the change resulted in an increase or decrease in security.

CMPFLDN
This overriding output format is intended for a value defined as COMPARE_CHANGES. It shows the name of the changed fields. Another way to use this output format is as a method to display the first column of the CMPCHG4 format.

Using the COMPARE_CHANGES formats: When using the four overriding formats CMPCHGV, CMPBASV, CMPCHGD, CMPFLDN, the individual rows reported correspond to each other by default. In the following example, the specification results shows information like that shown by the specification COMP_CHANGES(CMPCHG4), with smaller columns.

```
COMP_CHANGES(CMPFLDN,8)
COMP_CHANGES(CMPCHG,1)
COMP_CHANGES(CMPBASV,8))
COMP_CHANGES(CMPCHGV,8)
```

The output values are pieces of a coordinated group, just like in format CMPCHG4.

Compare the resulting output shown in the following example output to the output resulting for the CMPCHG4 format shown in the preceding example.

```
Fieldname                C Value-1                Value-2
CGGRPNM                    A                      G
CGGRPNM                    B                       E
CGGRPNM                                            F
DFLTGRP                    A                       F
```

The COMPARE_CHANGES field supports an overriding width. In the absence of any overriding format specification, the default width of the field is 80 characters, split over the three parts as 16/30/30. If an overriding width is specified, the widths of the individual columns are proportionally reduced or increased (and rounded appropriately). This is intended to allow an easy specification of COMP_CHANGES in a narrower format, while still providing useful information. If individual column width tailoring is required, or individual column selections are required, one of the CMP* overriding formats described above should be used.

An individual COMPARE_CHANGES column created by overriding format CMP* can have an overriding width. This is applied to the total column width in the report. To display the output horizontally, use the HORIZONTAL(length) output modifier. The overriding length field applies to an individual entry. The example shows the format specification and results:

```
/ COMP_CHANGES(CMPFLDN,80,HOR(8),PREFIX),
/ COMP_CHANGES(CMPBASV,80,HOR(8),PREFIX),
/ COMP_CHANGES(CMPCHGV,80,HOR(8),PREFIX)
```

```
Fieldname    DFLTGRP  CGGRPNM  CGGRPNM  CGGRPNM
Value-1      A        A        B
Value-2      C        G        E        F
```

In this example, the data shows the following:

- The value for DFLTGRP changed from A to the C.
- In the list of connect groups, the user was removed from the groups A and B and added to groups G, E, and F.

Using the LIST command

The following examples show how to use the format and output modifier parameters for the LIST command.

"Generating a group tree report" on page 834
"Generating separate lines using the newline operators" on page 835

Listing profiles using the profile key

One of the simplest requests is to list the class and name of selected profiles:

```
list class key
```

Changing the output length of a field

If you know the profile type you selected (for example CLASS=USER), you might want to modify the output length of the KEY field to 8 in order to get a concise listing of the users in your database:

```
select class=user
sortlist key(8) pgmrname instdata
```

By using SORTLIST instead of LIST, the profiles are sorted on the field values (in the order of the field names). This results in this example in a report sorted by RACF user ID.

Changing the display format

You can change the display to show data in different formats and field lengths. For example, if the first 3 bytes of the installation data contains bit flags, the default text format results in non-displayable characters that might disturb the printer. In this case, you can display the bit flags in hex. You might also want to specify the maximum length to be displayed. In this example, the correct field length is 6 bytes as shown in this LIST statement.

```
list key(8) instdata(6,hex)
```

Changing a column header

The column header can be changed by including a quoted string in the output name modifier list:

```
sortlist key(8) instdata('Personnel number')
```

The column header can be combined with length and format modifiers in any order. For instance, to add an output display length:

```
sortlist key(8) instdata(16,'Personnel number')
```

Listing the standard access list

To list the standard access list of resource profiles as well as the owner field and universal access, one might specify:

```
list class key owner userid useracs uacc
```

Displaying the access list using the ACL keyword

To display a combined standard access list and conditional access list, use the ACL keyword:

```
newlist
  select class=dataset, key=sys1.**
  sortlist class key owner acl
```

Including user information in the access list

To include the programmer data in the access list, one can use an indirect reference to the USER profile:

```
newlist
  select class=dataset, mask=sys1.**
  sortlist key owner acl acl:pgmrname
```

The users' installation data could have been included using ACL:INSTDATA.

Displaying the resolved access list

To show **all** user IDs that have access to a resource via the ACL, and calculate the actual access level of each user, use the ACL keyword with the RESOLVE format:

```
newlist
  select class=dataset, key=sys1.**
  sortlist class key owner acl(resolve)
```

As an alternative, the EXPLODE output modifier could have been used to display all the ways the users have been granted access. Using the EFFECTIVE output modifier would have summarized the actual access just like RESOLVE, but also included implicit access due to e.g. group operations.

Generating profile commands

To generate a command for each profile selected, you can use the string parameter of the list command. You can redirect the output to any file, for instance to CKRCMD. For instance, if you want to give every TSO user a permit to a specific account number:

```
newlist ddname=ckrcmd nopage
   select class=user, tso  /* all profiles with TSO segment */
   list 'PERMIT TSOACCT CLASS(ACCTNUM) ID(' | key(8) | ')'
```

The NEWLIST NOPAGE parameter can be used to suppress page headers when generating commands.

Generating repeat group commands

To generate a command for each repeat group entry of a selected profile, you can use the string parameter of the list command in combination with the RETAIN keyword of PRINT/NEWLIST. You can redirect the output to any file, also to CKRCMD. For instance, if you want to copy the class authorizations of a user to a different user:

```
newlist ddname=ckrcmd retain nopage
   select class=user, profile=USER1
   list 'ALU USER2 CLAUTH(' clname ')'
```

The preceding example would generate one RACF command for every authorized class. As an alternative, you could use the HORIZONTAL output modifier to generate just one command for each user, as demonstrated in the following example:

```
newlist ddname=ckrcmd nopage
   select class=user, profile=USER1
   list 'ALU USER2 CLAUTH(' clname(horizontal) ')'
```

The NEWLIST NOPAGE parameter can be used to suppress page headers when generating commands.

Generating a group tree report

The following example generates a simple group tree report; for each group, the group name (KEY) and installation data are displayed. The TREELINE field is sorts the groups in the proper order and the INDENT output modifier displays each group name at the proper offset. The DEPTH field must be present, since it is used by INDENT. Because a group name can be up to eight characters long, this example can handle groups up to a depth of 32 characters.

```
newlist type=racf
   select class=group
   sortlist treeline(nondisplay) key(40,indent(depth)) depth(nondisplay),
            instdata
```

Generating separate lines using the newline operators

To generate separate lines without changing the order of the values of repeated fields, you can use the soft newline operator '/n'. You can see this in the following queries.

When no newline operators are specified, repeated fields are shown as follows:

```
newlist
sortlist fieldA fieldB fieldC fieldD
```

Results in:

```
valueA1 valueB1 valueC1 valueD1
valueA2 valueB2         valueD2
valueA3
```

A normal newline operator '/' will first print the repeated fields before it with all their values, and then the fields after it:

```
newlist
sortlist fieldA fieldB / fieldC fieldD
```

Results in:

```
valueA1 valueB1
valueA2 valueB2
valueA3
valueC1 valueD1
        valueD2
```

A soft newline operator will keep the order of the values intact:

```
newlist
sortlist fieldA fieldB /n fieldC fieldD
```

Results in:

```
valueA1 valueB1
valueC1 valueD1
valueA2 valueB2
        valueD2
valueA3
```

MARGINS

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command sets the margins for reading the SYSIN file. The command can be abbreviated as MARGIN . The command must be followed by two decimal numbers separated by a comma and enclosed in parentheses.

```
MARGINS(nn,mm)
```

The first number gives the starting column for the text to consider (the first column is column number 1). The second number gives the last column to be read. Both numbers must be in the range 1 to 255, and the first number cannot be greater than the second number.

The default is dependent on the input LRECL and RECFM. For an LRECL=80 RECFM=F file (the MVS/JES2 default for inline SYSIN files), the following margins column settings:

```
margins(1,72)
```

This default ignores line numbers in column 73 to 80.

Margins commands in included files/members apply to the included file/member itself. You can also use the MARGINS parameter on the INCLUDE command to set margins for included members and files. Margins statements in a JCL parm set the default margins for reading the SYSIN file.

MENU

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

This command exists only for backward compatibility.

This command causes interactive operation under ISPF. The parameters of the MENU command can be used to select a 'selection panel' for display. You only need to use this command if you are customizing the ISPF interface. Specifying a non-existing panel name causes the application to be terminated.

CFS= *panel*
Menu panel name to be displayed after reading system configuration information from all CKFREEZE files.

MERGE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•			

Use the MERGE command to perform a RACF database merge. The command starts a block with a special syntax. This block is ended with an ENDMERGE command.

Between the MERGE and ENDMERGE commands (inside merge scope) normal CARLa syntax does not apply.

Note: You cannot MERGE databases accessed by the zSecure network. However, you can MERGE remote UNLOAD files.

The MERGE command only supports the following commands.

DEFINE
For example used to define variables for use in SELECT and EXCLUDE commands or later NEWLIST reports.

INCLUDE/IMBED
To include another file containing commands.

MERGERULE
Changes the way the merge decisions are made as described in "MERGERULE" on page 838. This command can only be used within a MERGE/ENDMERGE block. The MERGERULE command

SELECT/EXCLUDE
To select profiles from the SOURCE database. Based on the selected profiles of the SOURCE database, and optional MERGERULE commands, the merge process automatically selects relevant profiles from the CURRENT database.

When specifying `SELECT` and `EXCLUDE` selection criteria for the merge process, only use fields from the `BASE` segment. If the `BASE` segment is selected, the entire profile is merged. If the `BASE` segment is not selected, the entire profile is skipped, even if all non-`BASE` segments are selected.

MERGELIST

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the `MERGELIST` command to merge output of a number of NEWLIST commands. Its primary purpose is in creating ISPF displays that have different detail displays accessible from a common overview display. Another application is combining information from more than one profile segment into a multi-line report for each profile.

MERGELIST causes all NEWLISTs up to an ENDMERGE statement to be combined in a single display. The records are merged according to SORTLIST sort order. The sort is done column by column from left to right, irrespective of the field name displayed in the column. LIST, SUMMARY, and DSUMMARY are not supported in a MERGELIST, only SORTLIST/DISPLAY.

A maximum of 255 NEWLISTs are supported between a MERGELIST/ENDMERGE pair. If more NEWLISTs are required, consider dividing them over two or more MERGELIST/ENDMERGE pairs. There is only one MERGELIST level; that is, MERGELISTs cannot be nested.

Most *print parameters* (such as output DDname) are taken from the first NEWLIST statement; the parameters from the next NEWLISTs are ignored. The exceptions to this are the ISPF second-level (repeat group / detail) parameters, (that is, TITLE, SUBTITLE, DETAILHELPPANEL) and modifier details; these are taken from the actual NEWLIST that generated the output.

When the first NEWLIST is suppressed, the entire MERGELIST is suppressed (except when there is no collation because LIST has been used). Reasons for suppression can be a mismatching SEGMENT=*segment*, ESM=*esm*, LICENSE=*productcode*, UNRESTRICTED, RDS, or NONRDS specification. For example, when you want to mix RACF-specific and ACF2-specific report output into one MERGELIST, you might want to include a dummy `NEWLIST TYPE=SYSTEM OUTLIM=0` at the start so that there is no ESM= effective on the MERGELIST level.

Notes:

1. SEGMENT=BASE on the first NEWLIST is considered safe.

2. Suppression of TYPE=RACF newlists can also occur because of SUPPRESS RACF or the absence of a RACF data source.

When running in a "real-time" context, (for example, as part of zSecure Alert), output is processed in intervals. If the input for a particular NEWLIST type has been exhausted, the NEWLISTs of that type are suppressed.

Whenever a secondary NEWLIST is suppressed only because the first NEWLIST is suppressed, a warning message is issued (CKR2335-CKR2338). The return code for messages CKR2335, CKR2336, and CKR2337 can be adjusted through OPTION MSGRC=.

NAME
Name for the mergelist. When FILEFORMAT=XML is specified, this name is required; it used as the XML element name for all records output by the member NEWLISTs (for example those between MERGELIST and ENDMERGE). All fields that form a common prefix for each member NEWLISTLIST/SORTLIST/SUMMARY statements will be output as elements for this MERGELIST XML element. If a member NEWLIST contains additional fields, a subelement named with NEWLIST NAME= will be present, too. For an XML example, see "FILEFORMAT" on page 781.

DD
ddname
FILE
F Output file to use as a default for the newlists between MERGELIST and ENDMERGE. When you have also used a FILEOPTION statement for this file you do not need to specify DD= and the desired print parameters on each NEWLIST between MERGELIST and ENDMERGE.

Example

The following example shows a simple MERGELIST/ENDMERGE combination. The external selection selects all profiles with key DEMO*. Inside the MERGELIST/ENDMERGE, a further selection is made into user and group profiles; the output is dependent on the profile type.

```
select mask=demo*
mergelist
 newlist type=racf
  select class=user
  sortlist key(8) '(User) ' owner pgmrname instdata
 newlist type=racf
  select class=group
  sortlist key(8) '(Group)' owner supgroup instdata
endmerge
```

MERGERULE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•			

The MERGERULE command can be used to alter the way that the merge process works. It can be used to set global merge options, which are used as a default, or to set local options, which apply to a specific user or group and related profiles.

The following diagram describes the MERGERULE syntax:

```
MERGERULE        DEFAULT / SOURCEID= / SOURCECLASS=
                 options
MERGERULE        DEFAULT
                 [ AUTHORITY= ]
                 [ CONNECT= ]
                 [ CKGRACF=|CNGRACF=]
                 [ DATA= ]

MERGERULE        SOURCEID=
                 [ AUTHORITY= ]
                 [ CONNECT= ]
                 [ DATA= ]
                 [ OWNER= ]
                 [ RENAME= ]
                 [ SUPGROUP= ]

MERGERULE        SOURCECLASS=
                 [ AUTHORITY= ]
                 [ DATA= ]

AUTHORITY=       LOW
                 HIGH
                 MERGESOURCE, SOURCE
                 CURRENT
                 FLAG

CONNECT=         IFUSER
                 IFGROUP
                 IFBOTH
                 IFANY
                 NONE

DATA=            MERGESOURCE, SOURCE
                 CURRENT
                 FLAG

CKGRACF=|CNGRACF YES
                 NO
```

The MERGERULE DEFAULT statement applies to the global merge options, which have lower priority than a local (user or group-specific) MERGERULE SOURCEID command. It can be used to specify the default authority used, the default connect settings used, and the use of CKGRACF in the command output file.

The MERGERULE SOURCEID statement applies to one or more users or groups and related profiles (based on high-level qualifier), and has higher priority than the default values. It can be used to set the authority used, the connect setting, to apply a specific owner or superior group, and to rename the id during the merge process.

The MERGERULE SOURCECLASS statement applies to one or more general resource classes, and has higher priority than the default values. It can be used to set the authority and/or other data settings used during the merge process. Its syntax rules and limitations are the same as those of the MERGERULE SOURCEID statement.

All options can be specified using parentheses and/or an equal sign. (A list of ids must be enclosed in parentheses). For example, the following commands are valid:

```
mergerule sourceid(sys1) authority=flag
mergerule sourceid=ibmuser authority(mergesource)
mergerule sourceid=(ibmuser,cicsuser) owner=sys1
mergerule sourceid(ibmuser,sys1) connect(ifany)
```

Abbreviations are not supported. You can specify parameters for the same id on multiple MERGERULE commands, as the previous example shows. You cannot specify the same parameter multiple times for the same ID.

The MERGERULE keywords are:

AUTHORITY
The AUTHORITY keyword is used to specify the policy used for the id, in those cases where a security-related choice between the source and the current system must be made.

HIGH
Grants the highest access/authority. May cause security problems because of excessive access, so use with care.

LOW
Grants the lowest access/authority. May cause existing access to be removed.

SOURCE
Copy the access/authority from the MERGESOURCE system.

CURRENT
Copy the access/authority from the CURRENT system.

FLAG
Try to fall back on a default policy (if this is a local policy), or on a built-in default. If no decision could be made, issue an error message.

CKGRACF
The CKGRACF keyword determines whether CKGRACF commands are to be generated to set fields that cannot be set by RACF commands.

YES
Generate CKGRACF commands.

NO
Do not generate CKGRACF commands.

CONNECT
The CONNECT option determines which user group connections are to be copied; as decision criteria, the selected state of the user and the group are used. The connect attributes copied depend on the AUTHORITY setting.

NONE
Do not copy any user group connection.

IFBOTH
Only copy a connect if both source user and source group are selected.

IFANY
Copy a connect if either source user or source group, or both, is selected. If only one side is selected, the other side must already exist on the current system; otherwise, the connect is skipped.

IFUSER
Copy a connect if the source user is selected. If the group is not selected, it must already exist on the current system; otherwise, the connect is skipped.

IFGROUP
Copy a connect if the source group is selected. If the user is not selected, it must already exist on the current system; otherwise, the connect is skipped.

DATA
The DATA keyword is used to specify the policy used when a non-security-related choice between the source and the current system must be made.

SOURCE
Copy the field from the MERGESOURCE system.

CURRENT
Copy the field from the CURRENT system.

FLAG
Try to fall back on a default policy (if this is a local policy), or on a built-in default. If no decision could be made, issue an error message.

OWNER
Set a new owner for the specified user or group id.

RENAME
The RENAME parameter renames a SOURCE id to the specified new CURRENT id. This can be used to change the name of a user or group during the recreate process. Related profiles, as based on the high-level qualifier, are also renamed.

SUPGROUP
Set a new superior group for the specified group id.

Effect of keywords

The effect of the parameters is the following:

- A MERGERULE SOURCEID=xx, SUPGRP, OWNER, or NEWNAME command has the highest priority. These override any other command, and built-in defaults.

  If one of these keywords is specified for one or more ids, it is either applied or leads to a fatal error.
- The CONNECT options determine which user group connections to copy. A MERGERULE SOURCEID=xx (local) has higher priority than a MERGERULE DEFAULT command (global).

  If the CONNECTS keyword is specified for an id, its effect is dependent on the selected status and type of the target: it applies only if the target is selected. If both user and group have a command that could apply, and both are selected, the command for the user is used.
- The AUTHORITY and DATA options are used when deciding on security attributes such as (group)special. A MERGERULE SOURCEID=xx option overrides a MERGERULE DEFAULT option. The same holds for a MERGERULE SOURCECLASS=xx option.

  If either keyword is used, it applies only to those cases where a conflict needs to be resolved. There is no way to specify security attributes or data attributes if there is no conflict, for example source-only, or source equals current.
- IBM Security zSecure Admin built-in (non-command determined) alternatives are used as a last resort, for example if no local or default option could be used to resolve the problem.

MOVE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•			

The MOVE command generates RACF commands for moving a user to a new group and for removing users, groups, and permits or notify fields from the data set profiles of the old group. In the presence of one or more CKFREEZE files, the move operation also generates commands to delete data sets covered by removed profiles, data sets not covered by any profile, and catalog aliases having the sourceid as HLQ (if the command is intended to move the user to a *holding group* before deleting the user.

Note: The MOVE command is only supported if you have IBM Security zSecure Admin installed and enabled.

The MOVE command does not issue any commands by itself. The generated RACF commands are written to the CKRCMD file. [6] To complete the MOVE operations, verify and confirm the commands in the CKRCMD file and then run them.

The MOVE command syntax is similar to the syntax for the COPY and REMOVE commands. The MOVE command is mutually exclusive with VERIFY STC.

When the MOVE command runs, the resulting messages are similar to those generated by the COPY and REMOVE commands except that these messages include the *Move* term instead of *Copy* , *Replace*, or *Delete*, except the non-RACF commands, which generate messages that use the term *Resource deletion:*.

The keys and members of RACFVARS profiles are by default interpreted as users and groups when they match a valid user or group id, and they are managed accordingly, unless you use the SUPPRESS MANAGERACFVARS command. A discrete first qualifier in the key of a STARTED profile is only interpreted as a user ID when it matches the specification in the STUSER field in the STDATA segment.

The resource deletion commands generated as a result of the MOVE command can include ALLOCATE and FREE commands to delete uncataloged data sets. These commands are acceptable to TSO but not directly to IDCAMS. You can exclude these commands by specifying SUPPRESS DELETEUNCATALOGED, which will list the VTOC entries concerned in the SYSPRINT (as kept).

For a comprehensive description of the resource Delete functions, see "REMOVE" on page 870 and "SUPPRESS" on page 932.

For more information, see the following sections:

- "MOVE command parameter descriptions"
- "Using the MOVE command" on page 845

MOVE command parameter descriptions

The MOVE command has two types of parameters: user and group processing parameters and parameters that are modifiers for the processing parameters.

User and group processing parameters

The following user and group processing parameters for the MOVE command are mutually exclusive on a single MOVE command. If you want to use more than one

6. Commands in the CKRCMD file can also be generated as the result of a MOVE, REMOVE, or VERIFY command or a PRINT DD=CKRCMD command.

of these parameters, specify one MOVE command for each parameter. These parameters are also mutually exclusive with the VERIFY PERMIT command.

PERMIT= *id*

To prepare for moving the user ID or group, generate commands to remove references to the specified *id* from the following resources: access lists, OWNER fields, NOTIFY fields, RESOWNER fields, STUSER and STGROUP fields, NODES members, certain APPLDATA fields, and functional positions in profile keys and members of the classes:

- DATASET
- DLFCLASS
- INFOMAN
- CICS: TCICSTRN, GCICSTRN, DCICSDCT, ECICSDCT, FCICSFCT, HCICSFCT, ACICSPCT, BCICSPCT, JCICJCT, KCICSJCT, MCICSPPT, NCICSPPT, PCICSPSB, QCICSPSB, SCICSTST, UCICSTST, CCICSCMD, VCICSCMD
- VM: VMMDISK, VMRDR, VMBATCH, VMCONECT, VMEVENT, VMXEVENT, VMCMD
- SURROGAT
- PROPCNTL
- PTKTDATA
- LFSCLASS
- JESJOBS, JESSPOOL
- NODES
- STARTED, FACILITY
- TMEADMIN

You can limit the scope of the PERMIT using the FROMGROUP, TOGROUP, , and ALLPERMIT parameters as well as the SUPPRESS DELDSD command.

During the reference removal process, the following processing applies:

- If you specify the FROMGROUP parameter, the program only removes references in data set profiles of the indicated groups. It does not remove any references in general resource profiles or other user or group profiles.
- If you specify TOGROUP, the program removes all references except from the indicated group, the subject user, and general resource profiles.
- Deletes references in STUSER, STGROUP, and RESOWNER fields. To change profile ownership, certain APPLDATA and NOTIFY fields are deleted as appropriate.
- Creates commands to delete access list entries.
- Removes NOTIFY fields unless you specify the NEWNOTIFY parameter indicating which user should replace the one to be removed.
- Profile ownership is changed based on the following criteria:
  - For group data set profiles, it change to the first qualifier, as changed by ICHCNX00.
  - For connect profiles, ownership changes to the owner set by the command DEFAULT OWNER= or to the system default SYS1 if this command is not present.
- For other profiles, NOTIFY fields are removed unless the NEWNOTIFY parameter is used to indicate which user should replace the one to be removed.

NOTIFY= *id*

NOTIFY performs a subset of MOVE PERMIT= processing that is limited to NOTIFY fields.

USER= *idlist*

The USER parameter removes one or more users from the groups that are specified by the FROMGROUP parameter, and also removes all references to the user in the data set profiles of those groups. The USER parameter specifies all processing for `MOVE PERMIT=` and also generates RACF commands to remove the user from its connect groups and to modify the user's default group as needed.

The value specified for the *idlist* can be a single user name or a list of user names enclosed in parentheses and separated by commas.

Modifier parameters for user and group processing

The following modifier parameters can be used to adjust the processing performed by the PERMIT, NOTIFY, and USER command options.

FROMGROUP= *idlist*

This parameter limits the scope of the removal to the groups specified in *idlist*, which can be a single group name, or a list of group names enclosed in parentheses and separated by commas. This limitation of scope also extends to the data set profiles of the group: removal of access lists, owner fields, and so on is only done for profiles belonging to one of the groups specified in the list, which are identified either by their first qualifier or the qualifier returned by ICHCNX00.

TOGROUP= *idlist*

This parameter specifies a group or list of groups (*idlist* to which the user is to be connected. These connections replace the connections to the groups the users is currently connected to. If the FROMGROUP parameter is specified along with the TOGROUP parameter, the connections replace the connections to the groups specified by the FROMGROUP parameter. If a list of groups is specified, the list must be enclosed in parentheses with each group separated by a comma.

The TOGROUP option also reduces the scope of removal to exclude the personal data set profiles of the user, the group data set profiles of groups in the TOGROUP list, and all general resource profiles. If the ALLPERMITS parameter is specified along with the TOGROUP opton, even the user's profiles and references in general resource profiles are removed. The specified group can be a current connect group; in this case no connect command is generated.

The TOGROUP parameter is required when you specify MOVE USER or MOVE PERMIT commands.

ALLPERMITS

This parameter is valid only if it is specified after the TOGROUP parameter. ALLPERMITS causes references in all profiles to be removed, except by profiles of the group(s) specified on TOGROUP. This includes the user's profiles and general resource profiles that would be omitted by TOGROUP. The intended use of the ALLPERMITS parameter is to move a user to a *holding group* before deleting it. Therefore, it implies the generation of IDCAMS commands to delete the data sets and catalog aliases for the user as well, unless you specified `SUPPRESS DELETEDATASETS` for the run. Also, see the REVOKE parameter.

NEWNOTIFY= *id*

This parameter indicates a replacement user ID to be used for NOTIFY fields processed by the user/group removal commands.

REVOKE

This parameter can be used to revoke the user ID as well as performing the other actions on the MOVE command. The primary use of the REVOKE

parameter is to remove a user ID and move it to a holding group prior to deletion in a command such as `MOVE USER=`*id* `TOGROUP= REVOKE`*hold*.

Note: All parameters can also be specified as parm(value) in addition to `parm=value`.

Using the MOVE command

The parameters and other options you use with the MOVE command depend on the context of the user ID you want to move and also where you want to move it. The following sections provide examples of using MOVE commands in different scenarios.

- "Moving a user to staging group"
- "Moving a user to another department"
- "Transferring NOTIFY to a different user"

Moving a user to staging group

The following example generates commands to remove all references to a user ID JONES from the database and move the user ID to a staging group.

```
move user=jones togroup=holddel allpermits revoke
```

When this command is issued, RACF commands are generated for the following task and written to the CKRCMD file where you can verify and confirm them before submitting them:

- Remove all profiles for the user ID JONES.
- If the necessary CKFREEZE files are supplied, remove all the data sets covered by the profiles as well as any data sets without any covering profile and catalog aliases having JONES as their HLQ (tape data sets only if they are cataloged and migrated), a
- Move the user ID to a holding group temporarily so it can be deleted later, for example after it has been removed from non-RACF user definitions.

The default group of the user is changed as necessary.

For details on the parameters used in the command, see "MOVE command parameter descriptions" on page 842.

Moving a user to another department

The following example generates commands to move a user to a new department.

```
move user=jones fromgroup=dept1 togroup=dept2
```

When this command is run, it removes all authorities of the user *jones* on data set profiles of the group, *dept1* and connects the user to the new group. All authorities on general resource profiles and personal profiles for *jones* remain intact.

For details on the parameters used in the command, see "MOVE command parameter descriptions" on page 842.

Transferring NOTIFY to a different user

The following example shows how to generate commands to transfer all NOTIFYs on the data set profiles of a group to another user. For example, you might use this command to transfer NOTIFY responsibilities when a user is on temporary leave.

```
move notify=jones fromgroup=dept1 newnotify=parker
```

In this example, the NOTIFY responsibilities for the user ID *jones* in *dept1* are transferred to the user ID *parker*.

For details on the parameters used in the command, see "MOVE command parameter descriptions" on page 842.

NEWLIST

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use this command to generate more than one report, ISPF table, or unload file in one CKRCARLA program run. You use this command in combination with the following CARLa commands: LIST, DISPLAY, SORTLIST, SUMMARY, or UNLOAD.

For more information, see the following topics:

- "Selecting, formatting, and sending report data"
- "Sorting report data"
- "NEWLIST syntax rules" on page 847
- "NEWLIST parameter descriptions" on page 847
- "Overview of NEWLIST types" on page 850
- "Example NEWLIST commands" on page 855

Selecting, formatting, and sending report data

For reporting, the NEWLIST command marks the beginning of a new report description. You follow a NEWLIST command with the commands that determine what data is included in the report, the report format, and whether it is shown on the screen or printed: OPTION, SELECT, EXCLUDE, LIST, SORTLIST, SUMMARY, DSUMMARY, or UNLOAD. You can specify default settings for report selection, output formats, and output destination by specifying these commands as input before the first NEWLIST command. During processing, these commands are processed first. You can override the default options by specifying a new setting after the NEWLIST command where the setting applies. With each NEWLIST command, the options are reset to the default settings.

Within a NEWLIST block, any print or selection options you specify must be specified *before* the LIST, SORTLIST, DISPLAY, UNLOAD, or SUMMARY command.

You can use the NEWLIST command to direct different selections of LIST or SORTLIST output to a separate output file. See the Option command for an example.

If the selection criteria you specify do not result in any records being selected for the NEWLIST, no output is created even if you have specified a title. As a result, you can create reports or ISPF tables that only show in a pop-up window when one of the NEWLIST selection criteria is matched. See the EMPTYLIST keyword in "OPTION" on page 856 for details.

Sorting report data

When you create reports, you can direct the output for each NEWLIST statement to a separate file or direct all the output to the same file.

- If you direct the NEWLIST output to separate files, use LIST command to create the report. Each file contains the report output for the associated NEWLIST.

- If you direct the output from multiple NEWLIST statements to the same file, use the SORTLIST command on the NEWLIST statements instead of the LIST command. When you use the SORTLIST command, the report data is organized by NEWLIST type.

  If you use the LIST command in this situation, the data is written as it is processed. As a result, the report data from different NEWLIST statements can be mixed together, depending on the sequence of the commands.

NEWLIST syntax rules

The following syntax rules apply to the NEWLIST command.

- You can abbreviate the NEWLIST command to NEW or N.
- Within a MERGELIST and ENDMERGE command pair, you can specify a maximum of 255 NEWLISTs statements.
- Outside of a MERGELIST, you can specify as many NEWLIST commands as you need. There is no limitation.
- The NEWLIST statement accepts almost the same parameters as the OPTION command. For more syntax information, see "OPTION" on page 856. The parameters accepted by are the same as for the OPTION command. For additional examples, see the OPTION, LIST, and SELECT commands.

NEWLIST parameter descriptions

The following parameters apply to the NEWLIST command.

TYPE= *type*
This parameter identifies the type of information to be used as input for the NEWLIST. The default NEWLIST type is TYPE=RACF. In addition to the predefined types, described in "Overview of NEWLIST types" on page 850, all types created with the DEFTYPE TYPE=*type* command are accepted.

CMD
Issue each line of the LIST or SORTLIST output in this NEWLIST as local only, immediate TSO commands instead of as file output, unless the CMDTOFILE option is active. See "CMDTOFILE" on page 857. This type is only supported for RACF commands, the IDCAMS DEFINE command, and DELETE commands. For those APF authorized commands to work, either the program must be run APF authorized, or it must run under TSO (program IKJEFT01 in the batch or interactively). The maximum command length supported is 4096 (because of RRSF).

When you specify this CMD, the command is run immediately on the system that is running zSecure. The command is not subject to SETUP CONFIRM settings, nor issued through the CKRCMD file. This has been designed to be used as part of zSecure Alert (zSecure Audit for RACF running as a subtask in the C2POLICE address space).

COMPAREOPT=*compareopt*
Specifies the name of the COMPAREOPT specification to use with specified NEWLIST. The value specified must match the name specified for a defined COMPAREOPT statement. You can also specify the value DEFAULT to use the default COMPAREOPT specification as long as the default COMPAREOPT statement has been established by use of the FUNCTION=BASE option on an applicable ALLOC statement.

DETAIL
This requests that the fields on the DISPLAY command are by default shown on the detail panel and not on the overview panel. You can override this value with one of the following general output modifiers: NODETAIL BOTH, MORE

or NONDISPL on the field level. Because a DISPLAY command must show output on the overview panel, you must specify at least one override.

ESM= *list*
This parameter can be used limit the scope of this NEWLIST to input complexes that have an External Security Manager of any of the indicated types. The list can be a type or a list of types, where type can be RACF, ACF2, TSS, or NONE. This parameter is ignored for NEWLIST TYPE=DASDVOL, which produces a single cross-complex report.

ISPFTAB= *name*
I=*name*
This sets the name to be used for the NEWLIST on the NEWLIST selection level (only shown when multiple NEWLISTs have resulted in an ISPF display, for those NEWLISTs). The name specified need not be unique in the run, so this parameter can be used to show a single relevant name to select from several alternative NEWLISTs (e.g., because of RDS, NONRDS, LICENSE=*list*, or ESM=*list* criteria). On the other hand, it cannot be used in a LIKELIST=*name* clause. See also NAME=*name*.

LICENSE= *list*
This parameter limits the execution of the query to those products covered by the product codes listed. This makes it possible to have one CARLa input stream that gives tailored output for each product/license, for example a single set of SMF queries for both zSecure Audit for RACF and zSecure Audit for ACF2. The SELECT/LIST statements are not processed if the query does not apply. However, the NEWLIST statement is processed, and can still cause an error on an uninstalled NEWLIST type, for example. To prevent this problem, put the query into a separate member and use the LICENSE= parameter of the IMBED command instead (this will skip parsing the member entirely).

The following table lists the product codes that correspond to IBM Security zSecure products.

Table 299. Product codes

ADMINRACF	zSecure Admin
ALERTRACF	zSecure Alert for RACF
ALERTACF2	zSecure Alert for ACF2
AUDITRACF	zSecure Audit for RACF
AUDITACF2	zSecure Audit for ACF2
AUDITTSS	zSecure Audit for Top Secret
TCIMRACF	Tivoli Compliance Insight Manager Enabler for RACF
TCIMACF2	Tivoli Compliance Insight Manager Enabler for ACF2
TCIMTSS	Tivoli Compliance Insight Manager Enabler for Top Secret
TCIMCICS	Tivoli Compliance Insight Manager Enabler for CICS
TCIMDB2	Tivoli Compliance Insight Manager Enabler for DB2
zsecure_visual_s	zSecure Visual

zSecure Admin and Audit corresponds to (ADMINRACF, AUDITRACF).

NAME= *name*
N=*name*
This assigns an identifier to the NEWLIST, which is required if this NEWLIST is to be referred to by a LIKELIST=*name* clause on a SELECT or EXCLUDE

statement. The name assignment must be unique in the run. The name is also reported in the print summary in SYSPRINT. It is also used for the NEWLIST on the NEWLIST selection level (only shown when multiple NEWLISTs have resulted in an ISPF display, for those NEWLISTs), unless ISPFTAB=*name* was specified to control this separately. This parameter is required when output is directed to an output file with FILEFORMAT=XML.

NODUP
Eliminate duplicate records, for example records with identical contents in the columns used in the NEWLIST. For repeated fields, only the first value in a repeated field is used in the comparison. In the case of a summary, NODUP applies both to the input to the summary (duplicates are eliminated before the summary) as to the detail level (duplicate lines are removed, but they are counted, for instance when summarizing a repeat group field). This option does not apply to LIST output, since that command outputs each line immediately and does not remember previous lines.

Note that duplicate output lines might still be present, because different values can look the same due to formatting or truncation.

PROFLIST= *name*
NOTPROFLIST=*name*
PROFLIST indicates that the selections made by this list should be further filtered to include only information for the profiles selected by the referenced NEWLIST. NOTPROFLIST indicates that the selections made by this list should be further filtered to exclude all information for profiles selected by the referenced NEWLIST. The *name* must have been defined by a prior NEWLIST NAME= statement. This can for instance be used to combine reports on segment information of profiles selected in another NEWLIST based on fields in the base segment. You must be aware that all information as selected by the SELECT and EXCLUDE statements in *this* NEWLIST is stored in-storage, and the filtering through PROFLIST or NOTPROFLIST takes place later. So you should make the SELECT as restrictive as possible, in spite of the fact that the output remains the same whether or not a SELECT is present. In many cases, using SELECT LISTLIKE would be a useful alternative. A NEWLIST can have only one PROFLIST or NOTPROFLIST specification.

RETAIN
This option causes all non-repeat group fields on a SORTLIST or LIST to be repeated for each line that is needed to list the contents of all repeat groups. It can for instance be used to generate a command for each occurrence in a repeat group. It can be overridden locally by means of the output modifier NORETAIN. the keyword has no effect on a DISPLAY, unless it is routed to file (and becomes equivalent to SORTLIST).

SCOPE= *id*
Limit the output of a NEWLIST type containing resource information to information inside the scope of authority of the specified id (which can be a RACF user ID, or a RACF group). The scope check does not take into account system-wide attributesSPECIAL, OPERATIONS, and AUDITOR, but it does take into account group-SPECIAL, group-OPERATIONS and group-AUDITOR. SCOPE is only valid for NEWLIST TYPE=RACF and TYPE=SMF. The scope check applies to the UNLOAD command only for NEWLIST TYPE=SMF.

SEGMENT= *segment*
Suppress the NEWLIST if the segment indicated is not defined in the RACF database templates. Field names in the LIST family of commands are searched first in the indicated segment. This is needed for field PROGRAM in the OMVS segment since PROGRAM is also part of a base segment, having different

properties. This option also changes the meaning of the D action command to generate a command to remove the segment only instead of the complete profile.

SNMP
Requests an SNMP trap to be sent for each record in the NEWLIST. The destination must have been set with SNMPTO= option. If this OPTION parameter has not been specified before the first NEWLIST statement or on the NEWLIST statement, then output defaults to file output as if DD=C2RSNMP had been specified. SNMP traps are requested with a line length of 1066: 32 for a variable name, 1 blank, and a maximum value length of 1023. SNMP is mutually exclusive with email and WTO. SNMP is supported only on z/OS.

SYSLOG
Requests a syslog trap to be sent for each record in the NEWLIST. The destination for the output must have been set using the SYSLOGTO= keyword for the OPTION command. If this parameter has not been specified before the first NEWLIST statement and is not present on the first NEWLIST statement, then output defaults to file output as if DD=C2RSYSLG had been specified. Syslog traps are requested with line length 2048 and UTF-8 encoding. SYSLOG is mutually exclusive with the SNMP, email, and WTO parameters. SYSLOG is supported only on z/OS.

WTO
Issues a multi-line Writer to Operator (WTO) message for each record in the NEWLIST. The WTOs are issued with routing code 9 (security) descriptor code 12 (informational). The number of lines is limited to 10 and the maximum line length is 70. If more than 10 lines are generated, message CKR1421 is output. The extra lines are not issued, but they do appear in the SYSPRINT. Make sure the NEWLIST output record starts with a regular message identifier. WTO is mutually exclusive with the SYSLOG, email and SNMP parameters.

The WTO message format is affected by the APF status of the program. When the program is operating in APF authorized mode–that is, started through CKRCARLX or C2POLICE programs–the program adds a '+' in front of the message ID to prevent spoofing messages that trigger unwarranted Automated Operations responses. The '+' is not added to message IDs that start with C2P1 through C2P8, inclusive. For information about the APF authorization, see Chapter 11, “Calling zSecure,” on page 689.

Overview of NEWLIST types

The NEWLIST types that can be used depend on the product. Table 300 lists all NEWLIST types and the products which provide support for each type. See the Usage guides for additional information.

Table 300. Support for NEWLIST types by product

Newlist type	Description	ADMIN	Audit for RACF	Audit for ACF2	Audit for TSS
ACCESS	Access Monitor records	•			
ACF2_CLASMAP	ACF2 CLASMAP (map SAF class to resource type)			•	
ACF2_FDE	ACF2 Field Definition Entries			•	
ACF2_INFO	ACF2 Infostorage entries			•	

Table 300. Support for NEWLIST types by product (continued)

Newlist type	Description	ADMIN	Audit for RACF	Audit for ACF2	Audit for TSS
ACF2_INFOLINE, ACF2INFOLINE	ACF2 Infostorage General Resource rules, loose rule entries			•	
ACF2_INFORULE, ACF2INFORULE	ACF2 Infostorage General Resource rules			•	
ACF2_LID, ACF2LID	ACF2 logonids			•	
ACF2_RULE, ACF2RULE	ACF2 data set access rules			•	
ACF2_RES_INFORULE	ACF2 resident resource rules			•	
ACF2_RULELINE, ACF2RULELINE	ACF2 data set access rules, loose rule entries			•	
AUDIT	Audit concerns for `NEWLIST TYPE=SYSTEM.`		•	•	•
AUTAB, ICHAUTAB	RACF Authorized Caller Table	•	•		
CICS_REGION, IMS_REGION, DB2_REGION	Region and subsystem information for CICS, IMS, and DB2	•	•	•	•
CICS_TRANSACTION, IMS_TRANSACTION	Transaction information for CICS and IMS		•	•	•
CICS_PROGRAM, IMS_PSB	Program information for CICS and IMS		•	•	•
CLASS	RACF Class Descriptor Table	•	•		
CONCERN_TEXT	Audit concern translation strings	•	•	•	•
CONSOLE	System Consoles		•	•	•
CSM	Common Storage Map		•	•	•
DASDVOL	System DASD Volumes		•	•	•
DEFTYPE	User defined data source	•	•	•	•
DSN	Data set names		•	•	•
DSNT, ICHRDSNT	RACF Data Set Name Table	•	•		
EXIT	System Exits and Tables		•	•	•
FIELD	Built-in field names for LIST/SELECT statements	•	•	•	
FIELD_OVERRIDE	List of output fields that have overrides specified.	•	•	•	•
IOAPP	I/O Appendages		•	•	•
IP_AUTOLOG	Autolog configuration for MVS started procedures to be started by the Autolog.		•	•	•
IP_INTERFACE	Interface configuration for TCP/IP stacks		•	•	•

Table 300. Support for NEWLIST types by product (continued)

Newlist type	Description	ADMIN	Audit for RACF	Audit for ACF2	Audit for TSS
IP_RULE	IP filter rule configuration		•	•	•
IP_NETACCESS	Network access control configuration of TCP/IP stacks		•	•	•
IP_PORT	Port configuration of TCP/IP stacks		•	•	•
IP_ROUTE	Route configuration of TCP/IP stacks		•	•	•
IP_STACK	TCP/IP stack configuration		•	•	•
IP_VIPA	Virtual IP Address (VIP) configuration of TCP/IP stacks		•	•	•
JOBCLASS	JES2 Job Classes		•	•	•
MEMBER	Library Change Detection		•	•	•
MERGE	Report on MERGE processing	•			
MOUNT	UNIX mount points		•	•	•
MSG	Message Processing Facility		•	•	•
PC	Program Calls		•	•	•
PPT	Program Properties Table		•	•	•
RACF, PROFILE	RACF profiles	•	•		
RACF_ACCESS	RACF access through permits and connects	•	•		
REPORT_AC1, R_AC1	REPORT AC1 output (authorized executable modules).	•	•	•	
REPORT_NONDEFAULT, R_NONDEFAULT	REPORT NONDEFAULT output (RACF profiles optionally with data sets)	•	•		
REPORT_OUTOFGROUP, R_OUTOFGROUP	REPORT OUTOFGROUP output (RACF profiles optionally with data sets)	•	•		
REPORT_PADS, R_PADS	REPORT PADS output (executable modules contional RACF access lists).	•	•		
REPORT_PROFILE, R_PROFILE	REPORT PROFILE output (RACF profiles optionally with data sets)	•	•		
REPORT_REDUNDANCY, R_REDUNDANCY	REPORT (NON)REDUNDANT output (RACF profiles optionally with data sets)	•	•		

Table 300. Support for NEWLIST types by product (continued)

Newlist type	Description	ADMIN	Audit for RACF	Audit for ACF2	Audit for TSS
REPORT_SCOPE, R_SCOPE	REPORT SCOPE output (RACF profiles optionally with data sets)	•	•		
REPORT_SENSITIVE, R_SENSITIVE	SENSITIVE output (RACF profiles or High-level qualifiers with data sets).	•	•	•	
REPORT_STC, R_STC	REPORT STC output (started task JCL procedures).	•	•	•	
ROUTER, ICHRFR01	SAF router	•	•		
RRNG, RNG, ICHRRNG	RACF Range Table	•	•		
RRSFNODE	RRSF Configuration	•	•		
SENSDSN	Sensitive Data Set Names		•	•	•
SETROPTS	Systemwide RACF Options in database	•	•		
SETROPTS_CLASS	RACF Class Settings in database	•	•		
SMF	SMF records		•	•	•
SMFOPT	SMF Subsystem options		•	•	•
SPT, ICHRIN03	RACF Started Procedure Table	•	•		
SUBSYS	MVS Subsystems		•	•	•
SVC	Supervisor Calls		•	•	•
SYSTEM	System options for MVS, RACF, TSO, SMF, HSM, DMS, JES	•	•	•	•
TEMPLATE	RACF Database Templates	•	•		
TRUSTED	Trusted users and the reasons for it		•	•	
UNIX	UNIX file directory entries	•	•	•	•
VSM	Virtual Storage Map		•	•	•

Table 301. Support for NEWLIST types by product

Newlist type	Description
AUDIT	Audit concerns for `NEWLIST TYPE=SYSTEM.`
AUTAB, ICHAUTAB	RACF Authorized Caller Table
CLASS	RACF Class Descriptor Table
CONCERN_TEXT	Audit concern translation strings
CONSOLE	System Consoles
CSM	Common Storage Map
DASDVOL	System DASD Volumes

Table 301. Support for NEWLIST types by product (continued)

Newlist type	Description
DEFTYPE	User defined data source
DSN	Data set names
DSNT, ICHRDSNT	RACF Data Set Name Table
EXIT	System Exits and Tables
FIELD	Built-in field names for LIST/SELECT statements
FIELD_OVERRIDE	List of output fields that have overrides specified.
IOAPP	I/O Appendages
JOBCLASS	JES2 Job Classes
MEMBER	Library Change Detection
MERGE	Report on MERGE processing
MOUNT	UNIX mount points
MSG	Message Processing Facility
PC	Program Calls
PPT	Program Properties Table
RACF, PROFILE	RACF profiles
REPORT_AC1, R_AC1	REPORT AC1 output (authorized executable modules).
REPORT_NONDEFAULT, R_NONDEFAULT	REPORT NONDEFAULT output (RACF profiles optionally with data sets)
REPORT_OUTOFGROUP, R_OUTOFGROUP	REPORT OUTOFGROUP output (RACF profiles optionally with data sets)
REPORT_PROFILE, R_PROFILE	REPORT PROFILE output (RACF profiles optionally with data sets)
REPORT_REDUNDANCY, R_REDUNDANCY	REPORT (NON)REDUNDANT output (RACF profiles optionally with data sets)
REPORT_SCOPE, R_SCOPE	REPORT SCOPE output (RACF profiles optionally with data sets)
REPORT_SENSITIVE, R_SENSITIVE	REPORT SENSITIVE output (RACF profiles or High-level qualifiers with data sets).
REPORT_STC, R_STC	REPORT STC output (started task JCL procedures).
ROUTER, ICHRFR01	SAF router
RRNG, RNG, ICHRRNG	RACF Range Table
SENSDSN	Sensitive Data Set Names
SETROPTS	Systemwide RACF Options in database
SETROPTS_CLASS	RACF Class Settings in database
SMF	SMF records
SMFOPT	SMF Subsystem options
SPT, ICHRIN03	RACF Started Procedure Table
SUBSYS	MVS Subsystems
SVC	Supervisor Calls
SYSTEM	System options for MVS, RACF, TSO, SMF, HSM, DMS, JES

Table 301. Support for NEWLIST types by product (continued)

Newlist type	Description
TEMPLATE	RACF Database Templates
TRUSTED	Trusted users and the reasons for it
UNIX	UNIX file directory entries
VSM	Virtual Storage Map

Example NEWLIST commands

- "Selecting data outside and within the scope of a NEWLIST command"
- "Selecting data as placeholder using a NEWLIST"

Selecting data outside and within the scope of a NEWLIST command

This example shows a selection applying to all reports, and two NEWLISTs with a further subselection. This selection only works for NEWLIST TYPE=RACF, since a SELECT outside a NEWLIST scope *always* applies to NEWLIST TYPE=RACF processing. Refer to the next example for an alternative that is valid for all NEWLIST types. In addition, a title is generated common to all reports, and a subtitle that is different for each report.

```
print title='ABC Computer Services Inc, phone 234-17829'
select class=user
newlist subtitle='Users with system-wide SPECIAL attribute'
   select special
   sortlist key(8) pgmrname dfltgrp instdata
newlist subtitle='Users with system-wide OPERATIONS attribute'
   select operations
   sortlist key(8) pgmrname dfltgrp instdata
```

Selecting data as placeholder using a NEWLIST

This example shows a selection applying to one report that acts as a placeholder and does not generate any output, and two further NEWLISTs with a further selection. You can use this selection method with all NEWLIST types.

```
newlist type=racf outlim=0 name=users
 select class=user
 list key

newlist type=racf title='Users with system-wide SPECIAL attribute'
 select listlike=users special
 sortlist key(8) pgmrname dfltgrp instdata

newlist type=racf title='Users with system-wide OPERATIONS attribute'
 select listlike=users operations
 sortlist key(8) pgmrname dfltgrp instdata
```

Generating commands using the NEWLIST command

This example shows the use of the print keywords on the NEWLIST to create RACF commands to activate user auditing for users connected to a group external to the data center.

```
newlist dd=ckrcmd nopage
   select class=user congrpnm=external
   sortlist 'ALU' key(8) 'UAUDIT'
```

The NEWLIST NOPAGE parameter is used to suppress page headers when generating commands.

OPTION

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the OPTION command to modify global, print, and file options. For file option settings, the values you specify in an OPTION statement apply to all files. If you want to apply specific options to a specified file, use the FILEOPTION command. See "FILEOPTION" on page 779.

The effects of OPTION command settings depend on where the OPTION statement or command is specified in the CARLa program or command input.

- When an option setting precedes the first occurrence of a NEWLIST statement, it sets the defaults for all NEWLIST statements.
- When an option is specified in a BUNDLE statement, it specifies the settings for all NEWLIST statements that precede the matching ENDBUNDLE statement.
- When an option is specified in a NEWLIST statement or inside an OPTION statement within the NEWLIST statement, the options apply only to that NEWLIST statement.
- In a MERGELIST context, most OPTION and NEWLIST settings are taken from the first NEWLIST statement within the MERGELIST or ENDMERGE statement. The settings from the other NEWLIST statements are ignored.

ALLOWRESTRICT

When you specify the ALLOWRESTRICT keyword, CARLa queries can contain restricted fields in restricted mode. Messages CKR0170, CKR0217, CKR0384, CKR1276, CKR1382, and CKR1455 are still issued, but with a severity *4* warning message instead of a severity *12* syntax error message.

The ALLOWRESTRICT keyword is useful for running queries with restricted output fields and for complex SELECT statements with both restricted and unrestricted fields. Specifying this option setting means that you can generate some output in restricted mode. Without this option, a query with restricted fields fails because of syntax errors.

If you specify the ALLOWRESTRICT keyword in a NEWLIST statement that selects on restricted fields in restricted mode, the select operation processes the restricted fields like missing fields. In reports, the columns for restricted fields are empty.

In ISPF, issuing a query that results in no output being generated might be caused by the presence of a restricted field in the selection criteria. When no output is available, the ISPF selection panel shows the following message: CKRM948 No selections in scope. If the REQUIRED is also specified for any NEWLIST statement, the message only pertains to those NEWLIST statements. To prevent modification of a query in a manner that makes it ineffective in restricted mode, you can specify the ALLOWRESTRICT keyword for individual output fields.

You can suppress an entire query in restricted mode by specifying the UNRESTRICTED format modifier on the NEWLIST statement.

AUTODETAILSELECT

If a record display (not a summary level) has only one row/object, then the detail display is also automatically included. This behavior is not the default.

AUTOSELECT
If a summary level has only one line, then automatically select the line with S action command. This behavior is the default.

BCC= *email address list*
Sets the destination for blind carbon copy email messages. The *email address list* variable specifies the list of recipients that are confidentially copied on email messages. The value specified is a string that can be enclosed in any type of quotation marks or specified without quotation marks. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For more information about the restrictions, see 860. If omitted, no RFC 2822 field BCC: is added to the email.

BUNDLEBY= *variablename*
This option setting only applies within a BUNDLE...ENDBUNDLE group and is documented with the BUNDLE statement. See "BUNDLE" on page 733. Specifying the BUNDLEBY= value on an OPTION statement that precedes the first BUNDLE statement defines the default value.

CAPS
See "CAPS" on page 780.

CC= *email address list*
Sets the destination for carbon copy email messages. The *email address list* variable specifies the list of recipients that receive an email in addition to the primary recipients specified by the MAILTO keyword.

Specify a string value for the *email address list* with or without quotation marks. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For information about the restrictions, see 860. If omitted, the RFC2822 CC: field is not added to the email.

CMDTOFILE
Specify this option together with the CMD NEWLIST statement to test the CARLa query without actually issuing commands. The commands are written to the C2RCMD file. Verify that the C2RCMD file has been configured for a usable line length of 4096.

COMPAREOPT=*compareopt*
Specifies the default COMPAREOPT specification for all NEWLIST statements that do not explicitly specify the COMPAREOPT option. The *compareopt* value specified must match the name specified for a defined COMPAREOPT statement.

If a default COMPAREOPT statement has been established by the specification of the FUNCTION=BASE setting on an applicable ALLOC statement. You can use this default value by specifying value COMPAREOPT=*DEFAULT*.

ddname= *name*
DD=*name*
FILE=*name*
F=*name*
Specifies the ddname or file name for the report output. The following rules apply to the ddname specification.

- If the DDNAME keyword is used on the OPTION statement before the first NEWLIST statement, it applies to all NEWLIST statements. If the DDNAME keyword is used on a NEWLIST statement, it applies only to that NEWLIST statement.
- If the DDNAME keyword is also specified on a preceding FILEOPTION statement, the file options specified for the FILEOPTION are used.

- The following ddnames cannot be specified as a *name* value: CKRUNLIN, CKRUNLOU, STEPLIB, SYSABEND, SYSUDUMP, SYSMDUMP, CNRSAMP, CKRCARLA, CKRTSPRT, XMLIN, XMLOUT, CKRACF*, CKRSMF*.
- For some ddnames that are specified as the *name* value, the actual ddnames that are affected might be different if the file has been redirected with an ALLOC statement. This rule applies to the following ddname values: SYSPRINT, CKRCMD, CMDOUT, CNROUT, and CKR2PASS.
- When specified as a *name* value, the ddnames CKRCMD and CMDOUT are treated differently in the following respects.
  - A different command output file is used for each complex. This requires sufficient TYPE=CMDOUT files to be available using ALLOC statements.
  - TSO command line wrapping is activated and line continuation characters are used if the output record length is insufficient.
  - The sequence number fields are blank. Sequence number fields are the first 8 positions for variable record length files, and the last 8 positions for fixed record length files.

DETAILINHERIT
Echo the DISPLAY statement output for non-repeat group, non-detail fields for the currently selected object at the top of the detail display. This is the default setting for the DISPLAY output. The echo includes multiple two-line entries showing the column header line and first line for each summary-level display and the column header and first line of the object-level display output. Specifying the DETAILINHERIT keyword implies the DETAILSUMINHERIT option setting.

DETAILSUMINHERIT
Echo the DISPLAY summary and non-repeat-group fields of the currently selected object at the top of the detail display. The echo includes multiple two line entries showing the column header line and first line for each summary-level display and the column header and first line of the object-level display. Specifying the DETAILSUMINHERIT keyword implies the DETAILINHERIT option setting.

The DETAILSUMINHERIT option setting is automatically turned off when the NOSUMINHERIT keyword is specified.

DISPLAYTOFILE
When running in ISPF, treat the DISPLAY statement as if it were a SORTLIST statement. That is, write a batch report instead of creating an ISPF panel. The DISPLAYTOFILE keyword makes it possible to interactively test a query that can be specified for both ISPF and for a printed report, depending on an OPTION command in the preamble.

Note: In batch mode, a DISPLAY statement is always treated as a SORTLIST. For more information, see "SORTLIST" on page 918 and "DISPLAY" on page 778.

EGN
Format profile names as if enhanced generic naming were active. Generally, the EGN keyword option setting is not required. However, it is helpful if you have just converted from EGN to NOEGN because it can help identify profile names on the new system. The EGN keyword is not supported in restricted mode.

EMPTYLIST=HIDE
EMPTYLIST=SHOW
EMPTYLIST=*'string'*
EMPTYLIST=*"string"*

EMPTYLIST= *`string`*
EMPTYLIST=*:ISPFvar*
Specify the action to be taken when a NEWLIST statement does not generate any output, when the query returns no record selections for example. This option setting specifies both the inclusion of the NEWLIST report and the contents of the report itself. You can specify the following values.

Table 302. Empty NEWLIST output sets - Processing options

Processing option	Processing behavior
HIDE	• Suppress the empty table from the ISPF display panel. • In the SYSPRINT, do not show that the NEWLIST report was run. • Suppress the empty page from a batch report
SHOW	Displays panel or report to show that the NEWLIST statement was processed even if no output was generated. *SHOW* is the default setting for the serialization option. The display panel and report output is processed in the following manner. • Show the empty table from the NEWLIST statement on the ISPF display panel. • In the SYSPRINT, include the title for the NEWLIST report data. not show that the NEWLIST report was run. • Suppress the empty page from batch reports. In the ISPF interface, an empty table can be shown as a single line indicating zero (0) records or as a panel that only includes the header information.
SHOW stringvalue or SHOW ISPFVAR	An extension of the SHOW option, the text specified in stringvalue or by ISPFVAR is shown on the printed report.

The EMPTYLIST keyword can be abbreviated to EMPTY. For a bundle, the EMPTYLIST keyword applies to each bundle value.

ERRORMAILTO, EMT= *email address list*
If this keyword is specified in combination with the BUNDLEMAILTO keyword, reports for which no valid address is found are sent to the addresses specified in the list. This keyword also sets the addresses for the mail sender. If no FROM or SMTPMAILFROM value has been specified, the first address in this keyword also sets the default value for the SMTP MAIL FROM setting. In that case, this default value specifies the address for any error reports or delivery warnings the email server issues when routing the message. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For information about the restrictions, see 860.

FIRST_PER_NAME
Suppress a NEWLIST statement if it is preceded by another NEWLIST statement with the same name. Only the first NEWLIST statement with a particular name is processed. Any subsequent NEWLIST statement with the same name is suppressed. When a NEWLIST statement is suppressed for this reason, the CKR1232 is issued.

FROM= *email address list*
Sets the From: address list for an email.

Specify a string value for the *email address list* with or without quotation marks. The string content is interpreted as an address list conforming to RFC 2822,

with some restrictions. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For information about the restrictions, see 860.

If the FROM= keyword is omitted, the RFC 2822 From: field value is set to the value from the first available mail destination option. In priority order, the value is taken from one of the following keywords: SMTPMAILFROM, ERRORMAILTO, and REPLYTO.

HEADER=COLUMN
Display column headers. Do not use field prefixing. This setting is the default.

HEADER=NO, HEADER=NONE
Suppress column headers.

HEADER=PREFIX
Suppress column headers. Activate 'field comment' prefixing. See also “PREFIX” on page 800.

HELPDETAILPANEL= *panel*
DETAILHELPPANEL=*panel*
DETHELPPANEL=*panel*
Set the name of the ISPF help panel associated with a detail (repeat group) panel. The help panel is taken from the SCKRPLIB. The default is C2R&CKREREL.*nn*@0, where *nn* represents the NEWLIST type. See “FIELDS - Show CARLa fields available” on page 35.

For a NEWLIST type specified with a DEFTYPE statement, you can specify a default help panel name on the DETYPE statement. If you do not specify a value for the help panel, the value defaults to *C2R&CKREREL.NN@0*. The panel name is stored in ISPF variable CKRTHLPR. The panel name specified can contain the variable *&CKREREL*, which is replaced with *2* (for z/VM) or *3* depending on the ISPF level. but not in the first position.

HELPPANEL= *panel*
Set the name of the ISPF help panel associated with the overview panel. The help panel is taken from the SCKRPLIB. The default value is C2R&CKREREL.*nn*#0, where *nn* represents the NEWLIST type (see “FIELDS - Show CARLa fields available” on page 35).

For a NEWLIST statement type defined by a DEFTYPE statement, the default help panel name can be specified on the DETYPE statement. If you do not specify a value for the help panel, the value defaults to C2R&CKREREL.*NN*#0. The panel name is stored in ISPF variable *CKRTHLPP*. The panel name specified can contain the variable *&CKREREL*, which is replaced with *2* (for z/VM) or *3* depending on the ISPF level. but not in the first position.

LINELEN= *value*
LINELENGTH=*value*
LL=*value*
See “LINELENGTH” on page 782.

MAILfont size, MFS=
Sets the HTML font size for email. The default is 1. The HTML font size is a number in the range *1*–*7* corresponding to the following point sizes: 8, 10, 12, 14, 18, 24, and 26 point size if the browser default font is set at 12 point. The user can change the default point size.

MAILTO, MT= *email address list* **MAILTO=:***deftype.field*
Requests that the NEWLIST results are emailed to the addresses specified. This keyword must be either a string or an indirect reference to a field in a file

defined with the DEFTYPE command. See "DEFTYPE" on page 777 and "Field value manipulation" on page 760. With an indirect reference, the addresses found in each record specify the email recipients. The general RFC 2822 syntax states that an email address must include a local part, followed by an @ sign, followed by a host part, user_id@host.net for example. If the address contains other special characters for routing or other purpose, it must be enclosed in < and >, <@mailgate:user_id@host.net> for example. A list of email addresses can be specified, separated by commas.

The following restrictions apply to the RFC 2822 syntax.

1. Quotation marks are not supported within a quoted string within a phrase.
2. Line continuation within the RFC 822 string must conform to the CARLa string line continuation syntax–that is, continue on the first character of the next line. The line continuation does not conform to the RFC 822 line continuation syntax–that is, end with a comma and start the next line with a leading white space.
3. The canonized length of the phrase is limited to 512 characters. Canonized length means that white space is eliminated if it is not permitted by the RFC 821 protocol or reduced to one blank if it white space is required.
4. Phrase atoms equal to &system, &SYSTEM, or &System are replaced by the SMF system ID where the program is running.
5. Phrase atoms equal to &jobname, &JOBNAME, or &Jobname are replaced by the JES job name where the program is running.

The subject of the email is taken from the *title* or *toptitle* specified on the NEWLIST statement. This value overrides the DD and FILE specifications set previously.

Note: If *any* of the MAILTO keywords are specified, verify that the SMTPWRITER and SMTPCLASS options settings are valid, or include a C2REMAIL DD statement with an allocation to the SMTP writer. For more information, see "C2REMAIL" on page 702. You must also include at least one sender address on either the FROM, REPLYTO, SMTPMAILFROM, or ERRORMAILTO keyword. The email function of Security zSecure is not intended to be combined with the INFOPRINT email support introduced in z/OS V1R5.

MASKTYPE= *type*
Set the way filters are interpreted. The type can be either *EGN* or *ACF2*. If your product contains an ACF2 component and no RACF components, then the default setting is ACF2 masking. In the other cases, EGN masking is the default setting.

MAXP= *number*
MAXPAGE=*number*
PRTMAXP=*number*
See "MAXPAGE" on page 782.

MSGRC=(*msgno***, *level*)**
Change the severity of specific messages to the indicated value. Currently, this keyword is only supported for the following message numbers.

- *171* - Class not in descriptor table.
- *172* - ICHCNX00 problem.
- *438* - Storage shortage processing SMF.
- *2335* through *2337* - Warnings that the suppress options (for example, LICENSE=, ESM=, UNRESTRICTED) on the NEWLISTs within a MERGELIST seem to be incompatible.

- *2339* - Warning that the value for the SEGMENT parameter in a select clause in a RACF report is not known to the program.

The MSGRC keyword is only supported for the OPTION command.

MY_CCSID= *number*
Change the default EBCDIC encoding value of *1047* to the specified value. If you change the encoding, there is no guarantee that all program generated text can be read. For example, if you change the default encoding, output from the TYPE=SMF RECORDDESC NEWLIST might not be readable. The MY_CCSID keyword is only supported on OPTION statements.

NOACTION
Suppresses action characters on ISPF panels, even if the actions are available. When this keyword is specified, the action character column is not included in the panels. If this keyword is not specified, the default behavior is to analyze the permissions for each action character on a record-by-record basis. Based on the results, each record entry is made modifiable or non-modifiable. You can also use the NOACTION keyword for individual NEWLIST statements.

To turn off action characters for all NEWLIST statements in the run, specify the following setup command, `action characters allowed none`.

NOAUTODETAILSELECT
If a record-level display has only one row, do not automatically show detailed information. This behavior is the default setting because scrolling to the right on the detail does not scroll to the right on the record level display.

NOAUTOSELECT
Controls the selection behavior on summary level display panels that include only one summary line. The default behavior is to automatically select the summary line. Use the NOAUTOSELECT keyword to disable the automatic selection.

NODETAILINHERIT
Suppress automatic display of the non-detail line and its column header. Specifying this option gives the detail display more room, but leaves it to the query writer to show the object key somewhere on the display.

NODETAILSUMINHERIT
Suppresses repetition of summary information for the detail display. This behavior is implied when the NOSUMINHERIT keyword is specified

NOEGN
Format profile names as if enhanced generic naming (EGN) was *not* active. Profiles that would be supported by EGN but not by NOEGN can be found by searching for a colon (':'). This option can be helpful if you have converted profile names from NOEGN to EGN and are considering returning to the NOEGN format. You cannot specify this option in restricted mode.

NOMAIL
Turns off the email function for any NEWLIST statements that occur after this NOMAIL setting is specified. This setting turns off any default email setting specified by a preceding OPTION command.

NOMODIFY
For ISPF display panels, specify this option to make NEWLIST output read-only when it is initially shown. This parameter overrides the initial setting. After the information is shown, users can specify the MODIFY or SET MODIFY ON commands to make the display modifiable. The MODIFY setting in the application profile for the user ID is not changed.

NONULLS
See “NONULLS” on page 782.

NOPAGE
See “NOPAGE” on page 782.

NOSMTPTOFILE
Turns off SMTPTOFILE redirection for the NEWLIST. This is a local option that only applies to the current NEWLIST. If this option is specified, any output from the NEWLIST is sent by email.

NOSUMINHERIT
Disables echo behavior for the DISPLAY summary lines and headers for the currently selected object. By default, an echo is shown that includes two lines: the column header line and the first line for each summary-level display.

NOWARNING
Reset the return code to *0* when warning messages have been issued. If the internal return code is set to *4* or less as a result of warning messages, the return code is reset to *0* at the end of the CARLa run. This option is only valid on the OPTION command.

NOWTOFILE
Turns off WTOFILE redirection for the NEWLIST. This is a local option that only applies to the current NEWLIST. If this option is specified, any NEWLIST output is sent by WTO message.

NULLS
See “NULLS” on page 783.

OUTLIM= *n*
This halts output processing for subsequent LIST/SORTLIST/DISPLAY/SUMMARY command if the indicated number of records has been selected for output processing.

ONLYAT
Provides support for targeted deletion of data set profiles from nodes in an RRSF network if profiles are no longer in use by any other node in the system. The intent of the ONLYAT option is to prevent the accidental deletion of RACF database profiles that protect an existing resource.

Multi-system support can direct RACF commands through the RRSF network. In an RRSF configuration, deletion of a data set profile from any RACF database by a CARLa-generated command is not permitted if the profile is still in use by any RRSF node in the network. CARLa suppresses the generation of profile delete commands that are valid for some RRSF nodes but not all. You can override the default behavior and allow CARLa to generate profile delete commands that are directed at a specific node by using the ONLYAT option.

For this support to function correctly, system (CKFREEZE) images must be available for all systems being analyzed, either through an active zSecure Network Server connection, or by allocating them directly.

If the zSecure ONLYAT option **is not** specified, CARLa suppresses the generation of a DELDSD command if a data set profile is in use on any RRSF node in the network. A profile cannot be deleted as long as it is in use on at least one RRSF node.

If the zSecure ONLYAT option **is** specified, CARLa generates the DELDSD command that would have otherwise been suppressed and adds the ONLYAT keyword to:

- Allow deletion of a profile on a target RRSF node if the profile is no longer in use
- Prevent deletion of a profile that is in use on other RRSF-connected nodes

This keyword is specified in conjunction with the VERIFY PERMIT, VERIFY NOTEMPTY, and VERIFY ALLNOTEMPTY commands to add the ONLYAT parameter to generated RACF commands that support the ONLYAT parameter.

OUTPUTFORMAT=TEXT
OUTPUTFORMAT=EMAILDEFAULT
OUTPUTFORMAT=ATTACH

Specifies the method for including the results from a NEWLIST in an email. The following values are supported.

- TEXT includes the report inline as plain-text with limited HTML encoding. This is the only valid format for reports that are not emailed.
- ATTACH includes the report as an attachment. This is the default value for emailed XML NEWLIST data. This format is also required if UTF-8 encoding is specified.
- EMAILDEFAULT includes the report inline as MIME or HTML with limited HTML encoding. This is the default value for non-XML NEWLIST data.

OVERPRINT= *n*
OVP=*n*

See "OVERPRINT" on page 783.

PAGEALIGN= *value*

Ensures that the output from a NEWLIST statement for a specific BUNDLE value starts at a multiple of the *value* specified for the PAGEALIGN keyword. This behavior is achieved by generating empty pages at the end of the previous NEWLIST until the alignment is met. For example, if PAGEALIGN=4 is specified, the NEWLIST output can start on page *5*, *9*, or *13*, but not on page *6*. This feature can safely be combined with the PAGERESET keyword.

The PAGEALIGN= keyword is a normal OPTION setting that propagates to all NEWLIST statements. As a result, if the PAGEALIGN= keyword is specified on a BUNDLE statement, it applies to each NEWLIST statement within a specific bundle value. When applied to a NEWLIST statement outside of a bundle, the PAGEALIGN= setting applies only to that NEWLIST statement.

Note: If you specify the PAGERESET keyword in a stream of CARLa command input with multiple in combination with multiple PAGEALIGN= keywords with different values, the result might not be as expected.

PAGELENGTH= *number*
PAGELEN=*number*
PL=*number* **NOPAGE**

See "PAGELENGTH" on page 783.

PAGERESET

Reset the page number of NEWLIST output for a specific bundle value to *1* at the start of the report. You can safely combine this keyword with the PAGEALIGN= keyword on the *first* NEWLIST in the BUNDLE only, and *not* on the BUNDLE statement.

The PAGERESET= keyword is a normal OPTION setting that propagates to all NEWLIST statements. As a result, if the PAGEALIGN= keyword is specified on a BUNDLE statement, it applies to each NEWLIST statement within a specific bundle value. The best way to restart page numbering for each bundle value is to specify the PAGERESET on the first NEWLIST statement in the bundle rather than

specifying it on each NEWLIST statement within the bundle. When applied to a NEWLIST statement outside of a bundle, the PAGERESET setting applies only to that NEWLIST statement.

PREFIXLEN=*nn*
Specifies the length of the prefix headers for output from a NEWLIST statement. If this OPTION setting precedes the first NEWLIST statement, it applies to all output. Prefix headers can be included in both detail displays and print detail format output, by specifying the output modifier PREFIX or theNEWLIST option HEADER=PREFIX.

The following syntax rules and guidelines apply to the PREFIXLEN keyword.

- The minimum and default length for this value is 29.
- The maximum length for this value is *70*.
- You can specify the SYMBOLIC option to define a numeric character that represents the value as shown in the following example.
  ```
  PREFIXLEN=name|29
  ```
- If you specify a large value for the PREFIXLEN keyword, the space available for the variable output can become smaller if the value was specified with overriding length 0, which is interpreted as *until end of line* or *until end of screen*.
- You can also control the prefix length value from the NEWLIST clause in a LANGUAGE statement.

REPLYTO= *email address list*
Sets the *Reply-To:* address list for an email. The string value can be specified with or without quotation marks. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For information about the restrictions, see 860. If omitted, the RFC 2822 field *Reply-To:* is set to 'Reply-To: DontReply@AutoGenerated'.

In addition, the address list can serve as a default value for the MAILFROM and FROM keywords.

REQUIRED
This option only applies when running from the ISPF interface. If the REQUIRED option is specified for any NEWLIST statement, at least one of the NEWLIST statements with REQUIRED setting must select at least one record. If this criterion is not satisfied, you are returned to the selection panel with ISPF message CKR769 Nothing selected.

SERIALIZATION(*serialization-options***)**
Specify which measures the program must take to ensure data integrity for CKFREEZE and UNLOAD data sets. Also specifies the action to take when all required resources are not immediately available. For serialization to operate properly, all jobs involved must specify the same resource name. That is, all jobs must specify the same value for the ENQ request. All jobs must also access data sets under their true names. Do not use aliases because a successfully acquired alias does not guarantee that the data set is available under its true name. The following values can be specified for the serialization options.

ENQ(*qnames***)**
Serialization option to provide data integrity and input data availability by specifying that the program issue the appropriate ENQ request. You can specify the following subparameters to indicate the desired type of processing.

CKRDSN
The program issues a sysplex-wide ENQ with this QNAME for all CKFREEZE

data sets, UNLOAD data sets, and SMF data sets for processing. The ENQ is shared for data sets that are read-only. It is exclusive for data sets that the ENQ writes to. This method guarantees that no other process attempts to refresh an UNLOAD or read a CKFREEZE data set while the data set is being processed.

SYSDSN
The program issues a system-wide shared ENQ request with this QNAME for all data sets it processes except for the following types.

- Data sets allocated as TYPE=INPUT.
- CARLa input data sets like the CARLa script library.
- non-critical output data sets like SYSPRINT and SYSTERM

This ENQ request is intended to be specified in combination with the WAIT serialization option so that the program can wait until all required data sets are available. Alternatively, you can specify the SYSDSN keyword in combination with the FAIL serialization option. If all the data sets are not immediately available, an error message is issued and processing ends. Issuing an ENQ request for QNAME SYSDSN requires that the program be APF-authorized.

This option is mutually exclusive with the NOENQ keyword.

FAIL
This serialization option specifies that the program is to stop further processing if the data sets for which an ENQ is requested are not immediately available. This option is mutually exclusive with WAIT. If neither is specified, FAIL is the default.

MAXWAIT(*nn*)
This serialization option specifies the maximum time the program waits for the data sets for which an ENQ is requested to become available, in minutes. Supported values are in the range *1 – 59*, inclusive, with a default value of 5 minutes. The MAXWAIT setting is only effective when it is specified in combination with the WAIT serialization option.

NOENQ
Specifies that no ENQ requests are to be issued. This option is mutually exclusive with the ENQ serialization option.

UNIT
Specifies that dynamic allocation is not performed until a unit becomes available to satisfy the allocation request. This setting applies mostly to tape data sets. This option requires that the program be APF-authorized.

VOLSER
This serialization option specifies that, if need be, dynamic allocation is not performed until the required *volser* becomes available. It applies mostly to tape data sets. This option requires that the program be APF-authorized.

WAIT
Specifies that the program is to wait until the data sets specified in an ENQ request are available. This option is mutually exclusive with the FAIL serialization option. If the program is APF-authorized, specify the MAXWAIT serialization option to set a maximum wait time. An unauthorized program can only wait for the specified time period to expire.

By default, the program uses the following settings for the SERIALIZATION keyword: SERIALIZATION(ENQ(CKRDSN),FAIL.

ServerToken=*ServerToken*
Keyword that specifies the 8-character suffix for the name of the name/token pair used for locating the Program Call (PC) information for the zSecure Server. The value specified is prefixed by the value *CKNSERVE*. The default value for ServerToken is *PRODSERV*. If this keyword is not specified, the default value is used. Specifying a value for the ServerToken is only required if you are running multiple zSecure servers on the same system, or if the value for the zSecure server has been changed from its default value.

SETROPTS_REFRESH_ON_END
Generate interactive SETROPTS REFRESH commands for selected profiles at the end of the CARLa run. This option is only valid on the OPTION command.

SMTPCLASS= *sysoutclass*
See "SMTPCLASS" on page 783.

SMTPMAILFROM= *email address list*
Specifies the email address list for routing emails. The first address in the list sets the RFC (2)821 SMTP header MAIL FROM address for emails. Email servers along the delivery route send error reports and delivery warnings to the specified address. In addition, the full address list can serve as a default for the FROM address.

Specify the email address as a string enclosed with any type of quotation mark or specified without any quotation mark. The string content is interpreted as an address list conforming to the RFC (2)822 protocol, with some restrictions. For information about the restrictions, see 860. If omitted, the RFC 2821 field *MAIL FROM* is completed from the first available option in the order FROM, REPLYTO, and ERRORMAILTO. To send email, at least one of the following four options must have been specified: SMTPMAILFROM, FROM, REPLYTO, or ERRORMAILTO.

SMTPNJENODE= *nodename*
See "SMTPNJENODE" on page 783.

SMTPTOFILE
This option can be set to redirect email (SMTP) output. The default destination is DD C2RSMTP. Only output generated as the result of a MAILTO or BUNDLEMAILTO keyword is redirected. It is meant for testing purposes, to be specified preceding the first NEWLIST statement. If specified on or after a NEWLIST, it only applies to an email specification on that NEWLIST.

SMTPWRITER= *name*
See "SMTPWRITER" on page 783.

SNMPTO= *destination:port*
SNMPTO=(*destination:port***,***destination:port***, ...)**
If the SNMPTO= keyword specification precedes the first NEWLIST statement or on a NEWLIST statement that specifies the SNMP option, it determines the output destination for SNMP traps. If SNMPTO= is omitted, the default destination for SNMP output is the normal file output in file C2RSNMP by default.

The destination can be a name looked up through DNS or an IP address. The destination can be followed by an optional colon and port specification in decimal form. If the destination is an IPv6 address containing at least one colon character and it is followed by a colon and a port specification, enclose the value in square brackets. For example, [::1]:1169 where ::1 is the IPv6 address and 1169 is a port number. This specification is different from ::1:1169, where 1169 is the last part of the IPv6 address ::1:1169, and where no port specification is present. Square brackets around an IP address are optional if the address is not followed by a port specification or if the address is IPv4.

SYSLOGTO= *destination:port*
SYSLOGTO=(*destination:port,destination:port, ...***)**
If the SYSLOGTO= specification precedes the first NEWLIST statement or if it is specified on a NEWLIST statement that specifies the SYSLOG option, it determines the output destination for SYSLOG traps.

The destination can be a name from a DNS or IP address lookup. The default port is 514. For more information, see the SNMPTO= parameter description.

If SYSLOGTO= is omitted, the default destination for SYSLOG output is the normal file output in file C2RSYSLG by default.

SNMPTOFILE
Redirects SNMP output. The default destination is DD C2RSNMP. Only output generated as the result of an SNMP keyword is redirected. The SNMPTOFILE keyword is helpful for testing output.

Make sure the SNMPTOFILE keyword precedes the first occurrence of the NEWLIST statement. If specified on or after a NEWLIST statement, the keyword applies only to the SNMP specification for that NEWLIST statement. For this keyword, the RECFM and LRECL settings for the C2RSNMP file are used, which default to a logical line length of 132 bytes for printed output files. To simulate the line length used when writing SNMP traps, you need an effective line length of 1056 bytes and therefore you must specify values of RECFM=VB,LRECL=1060 for the C2RSNMP allocation.

SUMHELPPANEL= *panel* **HELPSUMPANEL=***panel*
Set the name of the ISPF help panel associated with the summary panel. The help panel is taken from the SCKRPLIB. The default is the value of HELPPANEL. The value is stored in ISPF variable CKRTHLPS. The panel name specified can contain the variable *&CKREREL*, which is replaced with *2* (for z/VM) or *3* depending on the ISPF level. but not in the first position.

SUMINHERIT
Echo the DISPLAY summary line and header of the currently selected object at the top of the record display. The echo includes a multiple of two lines: the column header line and first line for each summary-level display. It is on by default.

SYSLOGTOFILE
Redirects output to the default syslog file C2RSYSLG. You must specify this keyword before the first NEWLIST statement. Only output generated as the result of a SYSLOG keyword is redirected.

Use the SYSLOGTOFILE keyword to send syslog output to a file for testing. When you specify this keyword, the LRECL and RECFM settings for the C2RSYSLG file are used, which default to a logical line length of 132 bytes for printed output files. To simulate the line length used when writing syslog output, specify RECFM=VB,LRECL=2048 for the C2RSYSLG allocation. If you specify SYSLOGTOFILE on a NEWLIST statement, the redirection applies only to that NEWLIST statement.

TOPTITLE,TT
TITLE,T
SUBTITLE,ST
PAGETEXT
See "(TOP)TITLE" on page 783.

UNRESTRICTED
NONPADS
Specifies that the NEWLIST statement is only processed if the program is running

in unrestricted (non-PADS) mode. Otherwise, ignore the NEWLIST statement and the commands within its context. Because the commands are skipped, no error message is issued.

Note: You can use the ALLOWRESTRICT keyword to suppress output from restricted fields in restricted mode instead of suppressing the entire query.

WTOTOFILE
This option can be set to redirect WTO output. The default destination is DD C2RWTO. Only output generated as the result of a WTO keyword is redirected. Use the WTOTOFILE keyword for verifying WTO output during the test process. If this keyword precedes the first NEWLIST statement, the setting applies to all NEWLIST statements that do not specify the setting directly. If the keyword comes after the first NEWLIST statement, it only applies to a WTO specification on that NEWLIST statement.

Example - Defaults set by OPTION commands

The following command set the default ddname for the output from all NEWLIST statements to *MYREPORT*. It sets the default line length for all NEWLISTs to *64*.

```
option dd=myreport ll=64
```

When these options have been set, the output from the example OPTION statements shown in this code example might not behave the way you expect.

```
option dd=myrepor1 ll=64
option dd=myrepor2 ll=132
```

The first option command sets the default ddname for all NEWLIST statements to MYREPOR1 and sets the default line length to 64. The second, changes the default ddname to MYREPOR2 and the line length to 132. In effect, the first option command is ignored. When you specify these settings with the OPTION command, the settings apply to all subsequent NEWLIST statements. To specify different ddname and line length values or other file option settings for specific NEWLIST statements, use the FILEOPTION statement.

Example - Redirecting report data

You can generate a separate file containing the security profile information from Security zSecure, for postprocessing, with SAS for example. To accomplish this task with the NEWLIST statement, direct the LIST command output to a separate file as shown in the following CARLa statements.

```
newlist ddname=listout
  select class=user
  list key(8) pgmrname instdata
```

These commands generate a file populated with User profile information.

Example - titles

When you generate multiple reports, you can configure a different title for each report. The following example generates a report with the TOPTITLE, TITLE, and SUBTITLE keywords specified in combination with two NEWLIST commands. The OPTION settings specified outside the scope of a NEWLIST serve as a default for each new list.

```
OPTION TOPTITLE='ABC Computer services Inc, phone 234-17829',
      TITLE='Security zSecure report output'
NEWLIST
   OPTION SUBTITLE='Users with system-wide SPECIAL attribute'
   SELECT CLASS=USER, SPECIAL
   SORTLIST KEY(8) PGMRNAME DFLTGRP INSTDATA
NEWLIST
   OPTION SUBTITLE='Users with system-wide OPERATIONS attribute'
   SELECT =USER, OPERATIONS
   SORTLIST KEY(8) PGMRNAME DFLTGRP INSTDATA
```

PRINT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The PRINT command is equivalent to the OPTION command, except that it does not support non-print options like MY_CCSID, MSGRC, and SETROPTS_REFRESH_ON_END. For further information, refer to “OPTION” on page 856.

The PRINT command can be abbreviated as P.

REMOVE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•			

The REMOVE command generates RACF commands to remove users, groups, permits or notify fields. In the presence of one or more CKFREEZE files, the Remove operation also generates commands to delete data sets covered by removed profiles, data sets not covered by any profile, and catalog aliases having the sourceid as HLQ (migrated data sets only if cataloged and tape data sets not at all).

The REMOVE command does not issue any commands by itself. The generated RACF commands are written to the CKRCMD file.

Usage notes

- Commands in the CKRCMD file can also be generated as the result of the following commands: MOVE, REMOVE, VERIFY or PRINT DD=CKRCMD .
- If commands are being queued from the interface, then commands in CKRCMD can also be generated by overtyping, including the extra SETROPTS REFRESH commands.

To complete the REMOVE operations, verify and confirm the commands from the CKRCMD file, and then run them.

The command syntax for the REMOVE command is similar to the syntax for the COPY and MOVE commands.

When the REMOVE command runs, the resulting messages are similar to those generated by the COPY and MOVE commands except that they use the term

Remove or or Delete instead of Copy or Replace. Any IDCAMS commands created by the REMOVE command generate messages that use the term *Resource deletion:*.

The keys and members of RACFVARS. profiles are by default interpreted as users and groups when they match a valid user or group id, and they are managed accordingly, unless you run the SUPPRESS MANAGERACFVARS command. A discrete first qualifier in the key of a STARTED profile is only interpreted as a user ID when it matches the specification in the STUSER field in the STDATA segment.

The Resource deletion: commands might include ALLOCATE and FREE commands to delete uncataloged (non-VSAM) data sets. TSO supports these commands, but they cannot be issued directly to IDCAMS. You can exclude these commands by specifying SUPPRESS DELETEUNCATALOGED, which will list the VTOC entries concerned in the SYSPRINT as kept.

If a CKFREEZE file is specified and you do not want to generate any resource deletion commands, specify SUPPRESS DELETEDATASETS for the run. If you issue this command, the CKFREEZE file is not read unless other commands require it. Otherwise, DELETE commands are issued against all cataloged disk data sets and cataloged migrated or archived data sets covered by the profiles subsequently deleted. The actions are also issued against unprotected or inaccessible data sets that have the removed ID as the HLQ and the corresponding catalog aliases. The DELETE commands are generated with the PURGE option to override any expiration settings. As a general rule, the NOSCRATCH option is only specified where necessary. You can suppress the NOSCRATCH commands entirely using the SUPPRESS DELETENOSCRATCH command. Because zSecure does not automatically clean up VSAM inconsistencies or orphan NVRs. check the VSAM or VVDS inconsistencies message category if you must take these issues into account.

In case of shared DASD, the commands are generated for the current system and might not work correctly when submitted on a different system. In addition, as much configuration is removed as possible. For example, catalog aliases in inactive or remote master catalogs are removed. Be cautious when using the REMOVE command, particularly if there are unconnected catalogs. If you have partially shared DASD, make sure to supply additional CKFREEZE data sets to inform the run about the DASD that does not belong to the current system. You might have to do some additional work from another system later on with updated CKFREEZE data sets. For details on excluding specific volumes or catalogs and other information, see the "SUPPRESS" on page 932 command documentation.

For more information, see the following sections.

- "REMOVE parameter descriptions"
- "Using the REMOVE command" on page 874

REMOVE parameter descriptions

The REMOVE command has three parameter types: users/groups to be processed, modifiers for the processing parameters, and independent parameters.

- "User and group processing parameters"
- "Modifier for user and group processing" on page 873
- "Independent parameters for the REMOVE command" on page 873

User and group processing parameters

The following group of user and group processing options are mutually exclusive on any single REMOVE command. To use more than one of these parameters,

specify a separate REMOVE command for each parameter. In addition, these parameters are mutually exclusive with VERIFY PERMIT and VERIFY STC.

PERMIT= *idlist*

The value specified for the *idlist* can be a single user or group name or a list of user or group names that is enclosed in parentheses and separated by commas.

To prepare the users or groups specified in the *idlist* for removal, the PERMIT parameter generates commands to remove references to user and group IDs from the following resources: access lists, OWNER fields, SUPGROUP fields, NOTIFY fields, RESOWNER fields, certain APPLDATA fields, STUSER and STGROUP fields, NODES members, and functional positions in profile keys and members of the following classes.

- DATASET
- DLFCLASS
- INFOMAN
- CICS: TCICSTRN, GCICSTRN, DCICSDCT, ECICSDCT, FCICSFCT, HCICSFCT, ACICSPCT, BCICSPCT, JCICJCT, KCICSJCT, MCICSPPT, NCICSPPT, PCICSPSB, QCICSPSB, SCICSTST, UCICSTST, CCICSCMD, VCICSCMD
- VM: VMMDISK, VMRDR, VMBATCH

The scope of the command can be limited by the `FROMGROUP`, `TOGROUP`, and `ALLPERMITS` parameters as well as by the `STUSER` and `STGROUP` and `RESOWNER` fields, and to change profile ownership, `SUPGROUP` fields, certain `APPLDATA` fields, and `NOTIFY` fields as appropriate. Profile ownership is changed based on the following criteria.

- For group data set profiles, ownership is changed to the first qualifier, as changed by ICHCNX00.
- For connect profiles, ownership is changed to the owner set by the command `DEFAULT OWNER=` . The default is `SYS1`.
- For other profiles, NOTIFY fields are removed unless the NEWNOTIFY parameter is used to indicate which user should replace the one to be removed.

NOTIFY= *id*

The NOTIFY parameter specifies a subset of `REMOVE PERMIT=` processing that is limited to NOTIFY fields.

USER= *idlist*

The USER parameter removes one or more users from the database or from a number of groups, including all references and the profiles used only for a single user. The groups are specified using the FROMGROUP parameter. The USER parameter specifies all processing for `REMOVE PERMIT=` and also generates the RACF commands to remove users from their connect groups, delete the user profiles if requested, and modify the default groups of the users as needed.

The value specified for the *idlist* can be a single user name or a list of user names that are enclosed in parentheses and separated by commas.

GROUP= *idlist*

The GROUP parameter removes one or more groups from the database, including all references and profiles used only for a single group. The GROUP parameter specifies all processing for `REMOVE PERMIT=` and also generates the RACF commands to remove users from groups, delete group profiles if requested, and modify default groups of users as needed. However, GROUP parameter processing does *not* automatically delete user profiles if a group is

the last remaining group for a user. For these types of user profiles, the remove commands generated will fail when they are run.

The value specified for the *idlist* can be a single user name or a list of user names that are enclosed in parentheses and separated by commas.

Modifier for user and group processing

The following parameters can be used to adjust the processing performed by the user and group processing parameters described in "User and group processing parameters" on page 871.

FROMGROUP= *idlist*
The FROMGROUP parameter limits the scope of the removal to the groups specified in *idlist*. The value specified for the *idlist* variable can be a single group name or a list of group names enclosed in parentheses and separated by commas. This limitation of scope also extends to the data set profiles of the group: removal of access lists, owner fields, and so on, is only done for profiles belonging to one of the groups in the list (either by their first qualifier or the qualifier returned by ICHCNX00).

TOGROUP= *idlist*
The TOGROUP parameter limits the scope of removal for a specified group or list of groups to exclude the personal data set profiles for a user, the group DATASET profiles for groups in the TOGROUP idlist, and all general resource profiles. The value specified for the *idlist* can be a single group name or a list of group names enclosed in parentheses and separated by commas. The TOGROUP parameter is only valid with the `REMOVE USER=` command. This parameter specifies a group (or list of groups enclosed in parentheses and separated by commas). If the ALLPERMITS parameter is added, the profiles and references for the user in the general resource profiles are also removed.

ALLPERMITS
This parameter is valid only when specified after the TOGROUP parameter. The ALLPERMITS parameter causes references in all profiles to be removed, except for those profiles for group(s) specified in the TOGROUP parameter. This includes removing the profiles and general resource profiles for the user that would not be removed if the ALLPERMITS parameter is not specified. The main use for the ALLPERMITS parameter is to move a user to a *'holding group* before deleting it permanently. See the REVOKE parameter description.

NEWNOTIFY= *id*
The NEWNOTIFY parameter indicates the replacement user ID to be used for the NOTIFY fields processed by the user/group removal commands.

REVOKE
The REVOKE parameter can be used on the REMOVE USER= command to revoke the user ID as well as performing the other actions on the REMOVE command.

Independent parameters for the REMOVE command

The following REMOVE options are independent functions.

REDUNDANT
The REDUNDANT parameter removes discrete data set profiles that are covered by a generic profile whose OWNER, WARNING, ERASE (where active globally), and audit settings are identical or can be considered *similar*. Access is considered *similar* if the access list contains the group to which the data set belongs with a lower level than present in GLOBAL DATASET member

&RACGPID.*. Access is also considered *similar* if a user ID is present on the discrete profile access list with an access that is also granted via one of the groups to which the user ID is connected. You can use the LIMIT DISCRETE and LIMIT GENERIC commands to process only discrete or generic profiles. See "LIMIT" on page 787.

REDUNDANT_PERMIT
Generate commands to remove permits to users that would have the same access just through their current set of connect groups. Processing is done separately for conditional and non-conditional access lists.

Warnings

- The REDUNDANT_PERMIT function assumes that list-of-group checking is active. If you do not have SETROPTS GRPLIST set, do not use this function.
- REDUNDANT_PERMIT does not take into account future connect revoke dates. That is, a user permit is deleted even if the connect to the group with the same access has a future revoke date set. User permits are deleted if both of the following are true.
  1. The access level is at most the access the user currently has for all groups connected to the user. (That is, the user permit does not lower the authority that would be granted through connect groups.)
  2. At least one other connect group gives exactly the same access when the connect group is not revoked at the database unload date.

Note: All parameters can also be specified as parm(value) in addition to parm=value.

Using the REMOVE command

The parameters and other options you use with the REMOVE command depend on the context of the resources you want to remove. Table 303 provides examples of using the REMOVE command. For details on the parameters specified in the examples, see "REMOVE parameter descriptions" on page 871.

Table 303. REMOVE command examples

Task	Code sample	Description
Removing references	`remove permit=jones`	Generates the commands to remove all meaningful references to the specific user ID or group *JONES* from the RACF database. For details on the PERMIT parameter, see "User and group processing parameters" on page 871.
Removing a user	`remove user=jones`	Generates commands to remove the user ID *JONES* from the database, including all personal profiles that belong to the user. For details on the USER parameter, see "User and group processing parameters" on page 871.
Removing redundant profiles	`remove redundant limit discrete`	Generates commands to remove redundant discrete data set profiles For details on the REDUNDANT parameter, see "Independent parameters for the REMOVE command" on page 873.

REPORT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•	•	•	

After performing a scan of the security database and optional CKFREEZE files, this command requests reporting functions based on analysis of the data. The reports are created after the scan finishes. This processing is in contrast to the LIST command that is performed *during* the scan.

The REPORT command requires much more memory than the LIST function. It is mutually exclusive with the MOVE and REMOVE commands. You can issue multiple REPORT statements when you run the program. However, there are some restrictions on using the parameters. For more information, see "REPORT parameters."

Report layout

The report layout is determined by the default layout for the specified NEWLIST type. If a REPORT *report* is requested and no corresponding NEWLIST TYPE=REPORT_*report* has been encountered, the program uses a default report layout that is compatible with earlier versions of the product. This layout is defined by the CARLa member CKRR *type*. This format does not support reporting on multiple complexes in one run. For a report that has complex names use the IMBED M=CKRL *type* instead, or the CKRD *type* to show data in ISPF. See "Report layouts" on page 252.

To avoid using the default report layout, the NEWLIST TYPE=REPORT_<*type*> must be present in the input CARLa statements before the REPORT <*type*> command.

REPORT parameters

The REPORT command provides parameters for selecting records to be included in the report based on criteria like profile type, access level, and scope. You can also add modifiers to the REPORT command to control the report output formats. For examples, see "Using the REPORT command" on page 883.

For information about parameter descriptions, see the following topics.

- "PERMIT, SCOPE, and ACCESS level"
- "Mutually exclusive REPORT parameters" on page 878
- "Data set, resource, and attribute options" on page 879
- "Report data sort order" on page 882
- "Page headers" on page 882

See the following parameter descriptions, for information about the parameters including descriptions, syntax, and any processing considerations.

PERMIT, SCOPE, and ACCESS level

Use the following parameters to report on resources by user of group ID and access level.

PERMIT= *ID*

Reports resources to which the specified user or group has access through an explicit reference in the access list or OWNER field, also known as *direct* access.

- The ACCESS parameter limits the report output to profiles that the *ID* can access at least at the specified level, ACCESS=UPDATE for example.
- You can create a report showing access to defined RACF users, who are otherwise not on the access list by specifying * for *ID*
- You can specify more than one PERMIT parameter.
- PERMIT is mutually exclusive with SCOPE.
- In a report run, you can specify multiple REPORT PERMIT parameters or multiple REPORT SCOPE parameters, but not a mixture of the two.
- If a NEWLIST TYPE=PERMIT command is not present before the REPORT command, then a single-complex default layout is included which is the CARLa member CKRRSCOP. See "Report layouts" on page 252.)

SCOPE= *ID*

Reports resources to which the specified user or group has direct or indirect access. The ACCESS parameter limits the output of the SCOPE parameter to profiles that the *ID* can access at least at the specified level, ACCESS=UPDATE for example. If *ID* is a user, access through connects is also listed. Access through universal access, data set global access table, and missing profiles with NOPROTECTALL is included with the correct exceptions, unless the reasons UACC, GLOBAL, and NOPROFILE are suppressed.

- If a profile has a warning attribute, it is considered equivalent to having ALTER access to the profile, unless the reason WARN is suppressed.
- Group-special, group-operations, and group-auditor attributes are propagated down the group tree to resources owned by owned groups and to resources owned by users owned by owned groups, unless the reasons GRPSPECIAL, GRPOPER,, GRPOPER,or GRPAUDIT are suppressed.
- The SCOPE parameter can use much more memory than the PERMIT= parameter. By specifying the value * for *ID*, a report is created showing the scope of jobs without a RACF user and other users that are given access based on the UACC. The number of profiles listed can be reduced by including the SUPPRESS REASON= command or by specifying the ACCESS parameter. (See "SUPPRESS" on page 932.)
- If you specify multiple SCOPE parameters, add PAGEBY=ID to the REPORT command so that the page header of the report lists the ID. If a NEWLIST TYPE=REPORT_SCOPE is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRRSCOP. See "Report layouts" on page 252.)

ACCESS= *level*

Specifies the minimum level of access. Use this parameter with the PERMIT or SCOPE parameter. You can also specify the ACCESS parameter for the AC1 and STC reports. The parameter applies globally for all REPORT options present and can only be specified once.Table 304 on page 877 lists the access levels you can specify, listed from highest level to the lowest level.

Note: For general resource classes where both the member class and the grouping class contain the same (member) resource, the SCOPE command processes the profiles the same way that RACF processes them; each profile is considered separately. This processing can result in the member resource having a different access level than the access level determined by a RACF FRACHECK command.

Table 304. Access levels and their meaning

Level	Meaning
OWNER	Authority through ownership.
QUALOWN	Authority based on the first qualifier of a data set profile. If the data set HLQ is a user ID, this user has QUALOWN authority. Otherwise, if the data set HLQ is a groupid, any user with group-special for this group has QUALOWN authority.
CREATE	CREATE authority - a more specific profile can be created.
ALTER-M	ALTER access on 'myself' - a user can alter some fields in their own user profile.
ALTER-P	ALTER access on a discrete profile (allowing you to issue PERMIT).
CKGOWNR	Access granted by the CKGRACF authorized component of IBM Security zSecure Admin through the CKG.SCP scope profiles. Exactly what can be changed further depends on CKG.CMD profile access. This can only be more access then standard RACF, not less.
ADMIN	Same as CKGOWNR.
CNGOWNER	Same as CKGOWNR.
ALTER-O	ALTER access caused by a group-operations attribute.
ALTER	ALTER access.
AD_READ	ADD, DELETE, and READ authority through a controlling profile in the FACILITY or XFACILIT or similar class.
ADD_DEL	ADD and DELETE authority through a controlling profile in the FACILITY or XFACILIT or similar class.
ADD	ADD authority through a controlling profile in the FACILITY or XFACILIT or similar class.
ADD-S	Limited ADD authority through a controlling profile in the FACILITY or XFACILIT or similar class.
CONTROL	CONTROL access.
D_READ	DELETE and READ authority through a controlling profile in the FACILITY or XFACILIT or similar class.
DELETE	DELETE authority through a controlling profile in the FACILITY or XFACILIT or similar class.
DELETE-S	Limited DELETE authority through a controlling profile in the FACILITY or XFACILIT or similar class.
UPDATE	UPDATE access.
READ	READ access.
READ-S	Limited READ authority through a controlling profile in the FACILITY or XFACILIT or similar class.
READLPA	The UACC does not allow READ, but the module can be read in the LPA.
LOADEXE	The UACC does not permit READ, but the module can be run, and it can be read using LOAD.
EXECUTE	`EXECUTE` access for running a module
COPY	A module can be read, but not run. If the operation does not depend on APF or library residence, then anyone can access its function by copying it to their own load library.
AUDIT	Audit access without any other access.

Table 304. Access levels and their meaning (continued)

Level	Meaning
HIDDEN	A PDS member or load module hidden by a similarly named member in a library in front of this library.
NONE	No access.

Mutually exclusive REPORT parameters

The REPORT parameters in the following list are mutually exclusive.

NONREDUNDANT
Lists all data set profiles that are different from a less specific generic profile, if any exists. These profiles are considered nonredundant because removing them changes the data set access. If they were redundant, removing them would have no effect on the access level. Profiles are non-redundant when they fit any of the following criteria.

- Profile is a top level generic profile.
- Closest less specific generic profile has different WARNING, effective, AUDIT, or ERASE [7]
- The access list is different from a less specific generic profile.

  Similar access lists are defined by one of the following conditions. 1) All users effectively have the same access on either profile. This condition might exist if the access list contains the group to which the data set belongs with a lower access level than the one specified in the GLOBAL DATASET member &RACGPID.*. 2) A user ID is present on the profile access list with an access that is also granted through one of the groups to which the user ID is connected.

In the report, the column marker **First reason** indicates why this profile was included in the report. If there are multiple reasons, only one reason is indicated. Text enclosed in hyphens does not indicate non-redundancy by itself, it is a marker to help interpret the report. For example, the text - candidate - identifies a profile that was compared with more specific profiles listed later in the report. The profile is considered a *candidate profile* because it can take over the function of a more specific, potentially redundant profile. See "RA.3.2 Non redundant - Data set profiles different from less specific profiles" on page 201. If a NEWLIST TYPE=REPORT_REDUNDANCY is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRRNONR. See "Report layouts" on page 252.NEWLIST TYPE=REPORT*report*

REDUNDANT
Lists the redundant profiles and the candidate profiles making them redundant. For the selected profiles, this parameter provides the same information reported by the NONREDUNDANT parameter. If a NEWLIST TYPE=REPORT_REDUNDANCY command is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRREDUN. See "Report layouts" on page 252.

NONDEFAULT
Report all profiles with non-default access control. Generally, each installation has its own defaults, which are part of the security policy. However, Security zSecure tries in a general way to report about profiles that deserve consideration. The following list describes the default conditions for different user and group data sets.

7. Erase-on-scratch is not considered if ERASE(ALL) or NOERASE global options are active. ERASESECLEVEL is not supported.

- For *User data sets*, default indicates the following. The owner field equals the first qualifier; there is no access list, and the UACC is NONE.
- For *Group data sets with a user as owner*, default indicates the following. The user ID is in the access list with ALTER, and the group data set qualifier, which is the first qualifier unless altered by ICHCNX00, is in the access list with UPDATE.
- For *Group data sets with a group as owner*, default means that the owning group is in the access list with ALTER.

If a NEWLIST TYPE=REPORT_NONDEFAULT is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRRNOND. See "Report layouts" on page 252.

OUTOFGROUP

Reports all outstanding permits on group data sets to users or groups outside that group (identified by the first qualifier unless changed by ICHCNX00). If a NEWLIST TYPE=REPORT_OUTOFGROUP is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRROUTG. See "Report layouts" on page 252.

For all report parameters (PERMIT=, SCOPE=, ACCESS=, NONREDUNDANT, REDUNDANT, NONDEFAULT, and OUTOFGROUP), you can limit the report to a subset of all profiles by using the SELECT or EXCLUDE statement. If you do limit the report, avoid excluding USER, CONNECT, GROUP, or GLOBAL profiles. In addition, to limit the report to only certain DATATSET profiles, you must ensure that all DATASET profiles are selected for the qualifier on which you want to report. For example, to report on the redundancy qualifier for the DATASET profile SYS1.PARMLIB, you must include all SYS1 DATASET profiles in the analysis.

Data set, resource, and attribute options

Use these options to include the following types of data in the report.

- The DATASET classes covered by the RACF profiles that were selected using other report parameters.
- The resource classes, other than the DATASET class, covered by the RACF profiles using other report parameters.
- Detailed profile information for the selected DATASET and resource profiles.
- Tape data sets that are currently in scratch status.
- Protection of load libraries that have the potential to circumvent the security system.
- The protection of load modules that are covered by program profiles present on the conditional access list of any data set profile.
- All data set profiles, GLOBAL DATASET members, and missing High-level qualifier (HLQ) generics that cover sensitive data sets that require protection. HLQ generics are of the form *user.*** or *group.***.

You can specify the following options combined with each other and with the previous options. To use these options, you must a currently selected CKFREEZE file for the input data source.

These options do not produce the correct results if you have excluded any of the following resources from the selection.

- Any profiles in the class DATASET starting with the same qualifier as the data set selected for analysis.
- The GLOBAL DATASET general resource profile.

- Any PROGRAM profiles for AC1.

The following list describes the parameters available for reporting.

DATASETS
DATASET
DSN
Report which data sets are covered by each RACF profile reported by the following REPORT parameters: PROFILES, SCOPE, NONDEFAULT, NONREDUNDANT, OUTOFGROUP, or SENSITIVE. For SENSITIVE profiles, the selection includes *all* data sets covered by generic profiles. Without this keyword, only the sensitive data sets are shown.

RESOURCE
RESOURCES
Report which resources other than data sets are covered by each RACF profile reported by PROFILES, or SCOPE. This parameter only applies to resources deemed sensitive. Sensitive resources can occur multiple times–once per access level that has a separate sensitivity. This keyword requires an AUDITRACF or AUDITACF2 entitlement.

SCRATCH
SCR
Reports on tape data sets that are currently in scratch status. You must specify this parameter in combination with the DATASET parameter. For CA1, this parameter applies only to the first data set name on tape, not to secondary data sets in a multi-volume complex. In the cases of TLMS and RMM, all files on a scratch tape can be present. This option is not supported in restricted mode.

PROFILES
PROFILE
Report the class, key, access list, owner, auditing, conditional access list, and erase status of all selected profiles for the class DATASET and the general resource classes. If a NEWLIST TYPE=REPORT_PROFILE is not present before the REPORT command then a single-complex default layout is included, CARLa member CKRRPROF. See "Report layouts" on page 252.

AC1

Report on the protection of load modules that have the potential to circumvent RACF. The following list shows the load module types considered for selection.

- The AC(1) members of all APF libraries with all their entry points.
- Modules in APF libraries that are present in the Program Property Table (PPT) with the BYPASS option or a *system key* (0-7).
- Modules in APF libraries that are present in the RACF authorized caller table with RACINIT or RACLIST authorization.
- Authorized I/O appendages.

The report includes the highest access to arbitrary users as given by the combined action of the following resources: PROGRAM profile UACC, DATASET profile UACC, link list residency, LPA residency, global access table, and the profile warning mode. You can specify the ACCESS=*level* parameter for selecting only those modules with a UACC of *level* or higher.

The report also shows the following information.

- All module occurrences with link list and LPA list concatenation numbers.
- In-storage MLPA residency.
- Base member names for alias entries.

- The RACF data set and program profile names.
- The authorizing attributes, and attributes extending the authorization to the TSO environment (AuthCMD, AuthPGM, and AuthTSF).

This report extends beyond column 132, and is truncated if using the default line length. However, the last field is the data set profile name. Depending on the length of your profile names, most profile names fit on the default line length. You cannot create the report for AC1 data if the product is operating in restricted mode. If a `NEWLIST TYPE=REPORT_AC1` is not present before the `REPORT` command then a single-complex default layout is included, CARLa member `CKRRAC1`. See "Report layouts" on page 252.

PADS

Report on the protection of load modules that are covered by program profiles present on the conditional access list of any data set profile. The output format is like the format described for REPORT AC1. You cannot create the report with PADS data if the product is operating in restricted mode. If a `NEWLIST TYPE=REPORT_PADS` is not present before the `REPORT` command then a single-complex default layout is included, CARLa member CKRRPADS.See "Report layouts" on page 252.

STC

Report on the protection of started tasks.

The report combines information from the following resources.

- Started Procedure Table ICHRIN03.
- The RACF database including the RACF 2.1 STARTED class.
- The JES2 procedure library concatenation in use for started tasks.
- The procedure library used by the master address space (MSTR subsystem).

You can specify the `ACCESS=`*`level`* parameter to select only those modules with a `UACC` of *level* or higher. You cannot create the report with PADS data if the product is operating in restricted mode. If a `NEWLIST TYPE=REPORT_STC` is not present before the REPORT command then a single-complex default layout is included, CARLa member `CKRRSTC`. See "Report layouts" on page 252.

SENSITIVE
SENS

Reports on all data set profiles, `GLOBAL DATASET` members, and missing the High-level qualifier (HLQ) generics that cover sensitive data sets that require protection. HLQ generics are of the form *user.*** or *group.***. The data sets being considered sensitive are included underneath each profile listed..

Table 305 lists the sensitive data sets by access level.

Table 305. Sensitive data sets for each access level

Access Level	Sensitive data sets
READ	RACF data sets RRSF data sets SMF recording data sets page data sets swap data sets JES2/JES3 checkpoint JES2/JES3 spool space JES2/JES3 parameter data sets system dump data sets TSO user attribute data set UADS

Table 305. Sensitive data sets for each access level (continued)

Access Level	Sensitive data sets
UPDATE	APF data sets LPA data sets SYS1.LPALIB SYS1.NUCLEUS JES2/JES3 STC and TSU procedure libraries MSTR parameter libraries MSTR procedure libraries MSTR VIO index STGINDEX HFS data sets (UNIX file systems) HSM control data sets MCDS, BCDS, OCDS DMS control data set DMSFILES DMS authorized parameter libraries DMS default parameter library CA1 tape management catalog TMC SMS ACDS, COMMDS, and SCDS data sets IODF data sets RMM parameter library and control data sets TLMS volume master file VMF ABR archive control file ACF
ALTER	ICF catalogs

If a `NEWLIST TYPE=REPORT_SENSITIVE` is not present before the REPORT command then a single-complex default layout is included, CARLa member `CKRRSENS`. See "Report layouts" on page 252.

Report data sort order

The output sort order can be given with the BY keyword. This setting only orders the default report layout. If you specify your own `NEWLIST TYPE=REPORT_`*`report`* statement, this keyword only defines the content of the field ORDER.

BY= *list*

Keywords indicating report sort order. *list* is a list enclosed in parentheses with the keywords separated by commas indicating one or more of the following sort fields. (The order given is the default sort order.)

ID

User or group to which data set belongs (but module name with REPORT AC1).

KEY DSN DATASET

Data set name (resource name).

MEMBER MEM

Member name (with AC1 PADS, and STC).

REASON

Reason (usable with NONDEFAULT and NONREDUNDANT).

Page headers

Use the PAGEBY keyword to provide page headers for reports. The BY keyword must precede the PAGEBY keyword. The BY keyword applies directly to the default report layout. If you specify your own `NEWLIST TYPE=REPORT_`*report* statement, this keyword only defines the content of the field PAGEBY.

PAGEBY= *key*

Keywords indicating report page separation. The *key* specified must be the first one in the `BY=` list. The *key* is one of the following fields.

ID
User or group to which data set belongs.

KEY DSN DATASET
Data set name (resource name).

MEMBER MEM
Member name (with AC1 PADS, and STC).

REASON
Reason (usable with NONDEFAULT and NONREDUNDANT).

Using the REPORT command

You can use the REPORT command to produce many different types of reports depending on the parameters you specify. The following examples provide a starting point for creating reports.

- "Example - Reporting by scope"
- "Example - Reporting by multiple scopes"
- "Example - Customizing the report scope"
- "Example - Reporting on sensitive data set protection"
- "Example - Reporting on nondefault profiles" on page 884
- "Example - Reporting on contents of selected profiles" on page 884

Example - Reporting by scope

This example shows how to request a report of all profiles that can be updated by anybody. It also requests a list of the data sets covered by each data set profile.

```
report scope=*, access=update, datasets
```

Example - Reporting by multiple scopes

This example shows how to request a number of scope reports, each starting on a new page. The PAGEBY parameter is required to show the user ID that is being reported on in the page headers).

```
report scope=user1, scope=user2, pageby=id
```

Example - Customizing the report scope

```
newlist type=report_scope,
toptitle='S C O P E   R E P O R T  -  A C C E S S: ',
st='Sorted on access, id, key and class'
 exclude access<=read
 sortlist access(page,toptitle) stamp(toptitle),
         id key(nondispl),
         class proftype key('Profile name' 44) volser,
         access via when

report scope=sysprog, scope=stgadmin
```

Example - Reporting on sensitive data set protection

This example requests a report on the protection of sensitive data sets. Note that the DATASET parameter must not be specified if you want to see only the sensitive data sets, and not all data sets covered by the profile also covering a sensitive data set.

```
report sensitive
```

Example - Reporting on nondefault profiles

This example shows how to report non-default profiles in a way suitable for distribution to RACF group owners. This is accomplished by requesting page separators for each identity (first qualifier). The page header changes when the PAGEBY value changes.

```
report nondefault, pageby=id
```

Example - Reporting on contents of selected profiles

This example requests a quick report on the contents of selected profiles.

```
select class=facility
report profiles
```

SELECT and EXCLUDE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The SELECT and EXCLUDE commands share the same parameters.

- The SELECT command selects records that match the conditions specified.
- The EXCLUDE command narrows the selection results by removing or omitting records that match the criteria in the EXCLUDE statement.

For example, you can use a SELECT statement to select all records in a particular resource class, the DATASET class for example. Then, you can use an EXCLUDE statement to remove DATASET profiles that do not have a profile name that matches a specified name pattern.

The SELECT command can be abbreviated as SEL or S. The EXCLUDE command can be abbreviated as EXCL or X.

The following example shows the basic syntax for SELECT and EXCLUDE statements.

```
select field=value [ field2=value2 ... ] [ field3==field4 ...]
select field5=value5
exclude field6=value6
```

Scope of SELECT and EXCLUDE command - global and local

The *scope* and *type* of a SELECT and EXCLUDE command depends on the context in which it is specified. Commands specified outside the domain of a NEWLIST statement have a global scope. Commands within the domain of a NEWLIST statement have a local scope.

Global scope - specified outside the domain of a NEWLIST

SELECT and EXCLUDE statements outside the domain of a NEWLIST statement have a global scope. These selections always apply to RACF profiles (RACF NEWLIST type). Any record not selected by global SELECT and EXCLUDE processing is invisible to the rest of zSecure Admin and Audit. Therefore, this selection not only restricts the input of all RACF NEWLIST statements, but also applies to intrinsically global commands like VERIFY, REPORT, COPY, MOVE, REMOVE, and MERGE. The selection also applies to NEWLIST commands that can be scoped like UNLOAD, SORTLIST and DISPLAY.

You can use a global EXCLUDE, specified with SETUP PREAMBLE for example, to determine the impact of removing profile(s) from the database. This type of EXCLUDE statement can circumvent structural errors or other unsupported conditions in the RACF database. See “SE.3 Setup - Preamble” on page 1654.

Usage notes

- Lookup operations and global commands like VERIFY might require more profile types as input than might be immediately obvious. Refer to the documentation for the global commands for details.
- For lookups, do not forget to include the profiles and segments being looked up.
- In restricted mode, only the QUAL= parameter can be used for global SELECT and EXCLUDE processing.

Local scope - specified within the domain of a NEWLIST

A SELECT or EXCLUDE inside the domain of a NEWLIST statement has local scope. Its type depends on the NEWLIST type. The default type is RACF. A local SELECT or EXCLUDE statement affects only the commands within the NEWLIST statement. Subsequent NEWLIST statements are not affected unless they are linked by PROFLIST, NOTPROFLIST, or LIKELIST statements.

Selection types

A SELECT or EXCLUDE statement evaluates a field or fields based on specified test criteria. The following types of tests can be used.

- "Selecting with a *field-value* compare"
- "Selecting with a *field-field* compare"
- "Selecting on field existence" on page 886
- "Selecting on manipulated fields" on page 887
- "Selecting based on previously specified criteria (LIKELIST)" on page 887

Selecting with a *field-value* compare

A *field-value* comparison selects or excludes records based on whether the value of the specified field matches the literal or constant value specified in the statement. This comparison type evaluates a field on the left of the relational operator against a constant value on the right of the relational operator, field=value for example.

Table 306 lists the different ways to specify search criteria for a field-value comparison. The operations available depend on the field and the values specified.

Table 306. Field-value selection - Relational operators, substring scan, and pattern matching

Operation	Valid in ...
= (equality)	all fields
<> or ¬= (inequality)	most fields
> , < , <= , and >= (greater than, less than, or equal to)	most text, numerical, date, and access level fields
: (substring scan)	most text fields *fieldname* =:*value*
filter (pattern matching)	most text fields

Selecting with a *field-field* compare

A *field-field* comparison selects or excludes records based on whether the contents of a field matches the contents of another field. For example, you might want to select all records that have a matching user ID owner and user ID default group. This comparison type compares the contents of a field on the left of a relational operator to the contents of a field on the right of the relational operator, field1==field2 for example. The relational operator,== in this example, is doubled

to differentiate a *field-value* compare from a *field-field* compare. In order to match, the field contents must have the same length and the same value.

Table 307 lists the relational operators for field-field comparisons.

Table 307. Field-field compare - relational operators

Normal operator	Field-compare operator
=	==
<>, ¬=	<<>>, ¬== **Note:** The ¬ is not doubled.
<	<<
>	>>
>=	>>==
<=	<<==

Usage notes Field compare operations are subject to the following restrictions.

- For character fields, the field contents is compared excluding trailing spaces.
- Substring operations and field lookups can be used on both sides of the doubled relational operator.
  - Both fields must have the same format, two character fields for example. Only the character, numerical, hexadecimal, and date formats are supported.
  - At most one of the fields can be repeated. That is, you cannot compare two (potentially) repeated fields.
  - The maximum field length is 255 characters.
  - You cannot use the substring scan operator (`=:`) because it is not supported.
-

Field-field comparison examples: The following example selects all RACF user profiles with a default-group not equal to the owner.

```
newlist type=racf
select class=user dfltgrp<<>>owner
sortlist key(8) dfltgrp owner pgmrname
```

The following example selects all SMF records for which the default group of the user is not equal to the user's owner.

```
newlist type=smf
select user:dfltgrp<<>>user:owner
sortlist user user:dfltgrp user:owner recorddesc
```

The following example selects all SMF records for which the first part of user's default group is not equal to the user's owner.

```
newlist type=smf
select substring(user:dfltgrp,1,4)<<>>substring(user:owner,1,4)
sortlist user user:dfltgrp user:owner recorddesc
```

Selecting on field existence

You can test field existence using the `EXISTS` and `MISSING` operations. These keywords can be specified in the following formats.

- `MISSING`(*field*)
- `EXISTS`(*field*)

Selecting on manipulated fields

In both *field-value* selection and *field-field* selection, you can change the contents of the fields in the compare statement before processing the comparison operation. The functions available for changing the contents are fully described in "Field value manipulation" on page 760. The following restrictions apply when you use indirect references in a SELECT statement.

1. In a NEWLIST TYPE=RACF context, no indirect references can be used.
2. Indirect references to a TYPE=*deftype* can only be used in a SMF NEWLIST context.

Selecting based on previously specified criteria (LIKELIST)

You can refer to the effective selection made in a NEWLIST statement in a later NEWLIST statement of the same type. When you define the first NEWLIST statement, specify a name for the statement using the NAME=*name* parameter. Then, you can refer to the statement by adding a LIKELIST=*name* clause on the second NEWLIST.

In the following example, this SELECT statement uses the selection criteria on the referenced NEWLIST to select the same records from the NEWLIST where the clause was added.

```
SELECT LIKELIST=name
```

You can use the LIKELIST function to configure the selection criteria for a number of queries in one place.

You can also use the LIKELIST function to restrict the domain of an overall report that includes multiple queries. For each NEWLIST you add the clause to the basic selection on each SELECT statement. For example, adding the following statement to a CARLa query selects all records with type 80 but restricts the effective selection to within the set defined in NEWLIST NAME=*name*.

```
SELECT TYPE=80 LIKELIST=name
```

Sometimes it makes sense to put such a concatenation in one place–in an SCKRCARL member for example– and make the NEWLIST selection statement configurable. That is, have the NEWLIST selection statement generated dynamically by the interface.

For example, several SMF CARLa scripts refer to a NEWLIST named *SMFSEL*, which is not included in the scripts. A dummy selection statement, NEWLIST NAME=SMFSEL is provided in CARLa script CKALFSEL. This script can be run by adding the following code either as is or with a modified CKALFSEL member. The first INCLUDE can also be replaced with a NEWLIST named *SMFSEL* that makes the desired selections.

```
INCLUDE MEMBER=CKALFSEL
INCLUDE MEMBER=actual report member
```

If you run such a configurable report without supplying a preceding, appropriately named NEWLIST selection statement, a CKR0403 syntax error occurs. Instead of adding the NEWLIST statement, you can also add a SUPPRESS MSG=403 command. In that case, the selection is regarded as void. That is, the LIKELIST clause selects all records just as the absence of a SELECT statement causes all records to be selected.

The following statement selects all records not covered in another query.

```
EXCLUDE LIKELIST=name
```

This type of statement can be useful to format specific records in one way and the rest of the records in another (standard) way.

The LISTLIKE keyword is an alias for LIKELIST.

Evaluating SELECT and EXCLUDE statement criteria

Each statement can include multiple test criteria. Test criteria are specified and processed based on the following implicit and explicit syntax rules.

- If several tests are specified in succession, a logical AND is implied. You can also specify explicitAND, OR, and NOT operators.
- Use parentheses to clarify and define the logical relation between AND and OR clauses.
- Parentheses are required with the NOT operator.
- If parentheses are not used, the effect of multiple explicit AND and OR operators is dependent on the NEWLIST type. TYPE=RACF is right-associative, which means that A and B or C must be read as A and (B or C). All other NEWLIST types are left-associative which means that A B or C must be read as (A B) or C.
- Use parentheses whenever there is ambiguity about which clause has priority.
- Implicit AND operators have a higher precedence than explicit AND and OR operators.
- Clauses on SELECT and EXCLUDE statements can be separated by blanks or commas.
- If a statement is to continue on the next line, end the line with a comma.

Processing multiple SELECT and EXCLUDE statements

Multiple SELECT and EXCLUDE statements can be specified in any context. Multiple statements are interpreted based on the following processing rules.

- All SELECT statements in any context are combined with a logical OR.
- All EXCLUDE statements in any context are combined with a logical OR.
- The SELECT statements are processed first. Records that match the selection criteria are included in the selection results.
- The records in the selection results are then processed based on the EXCLUDE statements. Any selected record that matches the criteria in an EXCLUDE statement is removed from the selection results. If no EXCLUDE statements are present, all selected records remain in the selection results.

The overall result is that, in any context, a record is selected if it matches the criteria in *any* SELECT statement and does **not** match the criteria in *any* EXCLUDE statement.

Valid fields for SELECT and EXCLUDE statements

The valid *fields* for SELECT and EXCLUDE statements depend on the type of information to be reported as specified by the NEWLIST parameter in SELECT or LIST statements. For NEWLIST TYPE=RACF statements, the valid fields depend on the RACF templates. In addition to the fields in the templates, a number of built-in fields and aliases are also valid. The valid fields for the RACF NEWLIST statement are described in "SELECT and EXCLUDE for NEWLIST TYPE=RACF" on page 889. For all other NEWLIST types, the fields that can be used are predefined.

Most fields can be used both for SELECT and EXCLUDE processing and for output. Some fields can only be used for selection or output. For an overview of the available fields for each report type, see Chapter 13, "SELECT/LIST Fields," on page 953.

Warning: Using selection criteria for different fields in the same repeat group might produce unexpected output. The unexpected results occur because the values for the fields in the selection criteria might have been found in different repeat group entries, and there might not be a single repeat group entry that has the combination of fields. For the ACL, CUSTOM_DATA, and USR repeat groups in the RACF NEWLIST (NEWLIST TYPE=RACF), you can use the ACL, CUSTOM_DATA, and USR selection parameters. See "SELECT/EXCLUDE ACL(...)" on page 890, "SELECT/EXCLUDE CUSTOM_DATA(...)" on page 890, and "SELECT USR(...)" on page 892. For other repeat groups, there is no simple way to select or exclude records based on different fields in the same repeat group entry.

You can use the DEFINE SUBSELECT command to include selected repeat group entries for some field types in display panels and reports. For more information, see "DEFINE" on page 750.

SELECT and EXCLUDE for NEWLIST TYPE=RACF

The fields you can specify as selection criteria for the RACF NEWLIST type are defined in the RACF templates. See "RACF: RACF profiles" on page 1124. You can also specify special, predefined fields to customize the SELECT and EXCLUDE statements for RACF profiles. For details, see the following sections.

- "Selecting by profile property"
- "Searching by profile name" on page 890
- "Searching by value in a specific field" on page 892
- "Selecting by built-in alias names" on page 893
- "Selecting profiles by resource class" on page 894

Selecting by profile property: Use the following parameters in NEWLIST TYPE=RACF statements to specify values for profile properties.

SEGMENT= *segment*
SEG=*segment*
S=*segmentpredefseg*
NO*predefseg*

Selects profiles that contain the indicated segment types. Only the segment is present in the selected record. A number of predefined segments can also be selected by specifying only the segment name. These predefined segments are: CICS, CDTINFO, CERTDATA, DCE, DFP, DLFDATA, EIM, KERB, LANGUAGE, LNOTES, NETVIEW, NDS, OMVS, OPERPARM, OVM, PROXY, SESSION, SIGVER, STDATA, SVFMR, TME, TSO, or WORKATTR.Prefixing the segment name with NO selects those profile segments that do not match the indicated segment. Selection on the absence of a segment is not supported.

SCAN=*val*
SCAN=(*val, val,...***)**

A string to scan for or a list of strings to scan for. The entire profile is scanned, unless the FIELD= parameter is also specified. If you use the FIELD= parameter, it must be specified before the SCAN= parameter. The SCAN= parameter is a fast way to restrict operations to certain profiles. If more SCAN parameters are coded on one SELECT or EXCLUDE clause or if a list of values is enclosed in parentheses, the scan matches if any of the SCAN values matches.

The following syntax rules apply to specifying values in the SCAN= clause.

- Use single, double or left quotations around the value if it contains lowercase, blanks, commas, or other special characters.
- A quoted string can be followed by a string conversion character C or T.
- The String conversion character C indicates case-sensitive. The string conversion character T indicates not case-sensitive.
- In a list of values, case-sensitive and not case-sensitive can be mixed.

Notes:

1. Hexadecimal string conversion is not supported.
2. The SCAN= parameter has been functionally replaced by the substring scan specification.

   fieldname =:*value*.

DB= *number*
Selects profiles based on the sequence number of the RACF database that originally contained them. The sequence number is defined in the RACF database name table.

RBA= *hex*
Selects profiles based on the Relative Byte Address value from the originating database. Together with the DB= parameter, this value describes exactly one profile. Its main use is to select profiles in situations where BAM conflicts are reported by IRRUT200, by excluding profiles that are in use but not present in the index for example.

Searching by profile name: The following parameters can be used for selections based on the profile name. They are mutually exclusive within a single SELECT/EXCLUDE clause.

ACL(*limitedACLsubselectclause***)**
Select on a combination of values in a single ACL repeat group entry. For the syntax of a 'subselect clause' and the fields generally supported in one, refer to “DEFINE” on page 750. The ACL subselect fields USER and GROUP are not supported for SELECT and EXCLUDE--use ID instead (when the id is encountered on the access list, the user or group profile it is to be matched against might not have been read yet, so the type is generally unknown).

BESTMATCH=*name*
Select the best matching profile as found with MATCH. This parameter performs the same function as the MATCH parameter but only shows the best matching profile(s). This is the profile that would end up on top if the result of a MATCH would have been sorted on SEARCHKEY. There are a few restrictions concerning the usage of BESTMATCH. This parameter can not be used in combination with the PROFILE / KEY, MASK / FILTER or MATCH parameter, can not be used in an explicit nor an implicit OR (multiple select statements), can not be used as a target for a LIKELIST, and can not be used for exclusion. BESTMATCH does not necessarily always result in one profile. All profiles that are equally 'best' will be shown.

CUSTOM_DATA(CUSTOM_DATA*subselectclause***)**
Select on the combination of key, type, and value in a single custom field entry. For the syntax of the CUSTOM_DATA*subselectclause* and the fields supported in one, see “DEFINE” on page 750.

MASK= *mask*
FILTER=*mask*
A mask for the profile key. Use **%**, *, and **.**** (enhanced generic naming). The

filter is *always* interpreted as enhanced generic, independent of the RACF database setting for EGN. If you specify a generic profile key here, this value matches generic and discrete profiles that are covered by this name. The meaning of a single * depends on the entity type.

- For data sets, a single * matches a qualifier with a maximum of 8 characters.
- For general resource profiles, a single * at the end of a FILTER or MASK statement, selects only a single qualifier (while in RACF it means any number of profiles).

The mask value can be specified with or without quotation marks. If no quotation marks are specified, the match processing is not case sensitive. If single, double or back quotation marks are specified, the match processing is case sensitive.

There is one extension to EGN matching. A single asterisk can also be used to match the first part of a qualifier. For example, **.*ABC.** finds qualifiers ending in ABC anywhere in the field, except for the first qualifier.

MATCH= *name*

Select all profiles that match the specified resource name. The result includes both discrete and generic profiles. However, the indicated bit and the volume serial numbers are ignored. The MATCH keyword is useful to determine the profiles that protect a resource if another profile is deleted. For grouping profiles, the match is on the member list of the grouping profile.

The following syntax rules apply to the MATCH specification.

- For case-senstive matching, specify the *name* in quotation marks (single, double, or backward). If case is not significant, specify the *name* without quotation marks.
- If a keyword is specified for a member class, the grouping class is automatically included. This syntax allows selection of all profiles that can protect a CICS transaction. See "Examples - SELECT and EXCLUDE statements" on page 908.
- If the MATCH and keywords are specified together, make them the first keywords in the SELECT or EXCLUDE statement or the WHERE clause.
- Specify the SEARCHKEY output field to sort the resulting profile names in order of best match.

PROFILE= *name*
PROFILE=(*name*, *name*, **...)**
KEY=*name*
KEY=(*name*, *name***)**

Selects a specific profile name. If you specify generic characters, the profile searched has exactly the key specified. Unlike other fields where generic characters imply a pattern match, generic characters for the KEY field are treated literally. To match more than one profile, you must use one of the following key words: MASK, FILTER, MATCH, or BESTMATCH. Use quotation marks (double or left) around the profile name, if it contains lowercase, blanks, commas, or other special characters (like /*). Names specified without quotation marks are converted to uppercase and only match uppercase profiles. Names specified in quotation marks or a list of names, even when the list consists of only one name, are interpreted to be of type T for text. The comparison of these values is not case sensitive. If you want the comparison to be case sensitive, specify the *name* as type C, *name*C for example.

USR(*USRsubselectclause***)**
Select on a combination of values in a single USR repeat group entry. For the syntax of a subselect clause and its supported fields, see "DEFINE" on page 750.

Searching by value in a specific field: Use the following parameters to search for values in a specific field.

*fieldname***=***vall*
*fieldname***<***vall*
*fieldname***>>***vall*
*fieldname***<=***vall*
fieldname **>=vall**
*fieldname***<>***vall*
*fieldname***(***vals***)**
Specifies a field name to be searched for in the profile. All normal comparison operators are supported. In addition, the format specifying a list directly following *fieldname* is equivalent to specify an equal sign.

fieldname
Specifies a name defined in a template, in a built-in alias, or by the keyword FIELDVALUE to indicate that the field name is given by the FIELD parameter. See "Alias names local to segments" on page 894.

vall
Specifies a value to search for in the specified field. Values can be specified using a pattern, a substring scan, or a list of values.

- To specify a pattern, use % or * in the search string.
- To specify a *substring scan*, start the string with the substring scan operator (:) that represents the SCAN operand. See "Selecting by profile property" on page 889 for more information about the SCAN parameter.
- To specify a list of values, separate each value with a comma and enclose the list in parentheses.

vals
Specifies a *value* to search for in the field specified, or a *list of values* separated by commas.

Usage notes:

1. A *pattern*, *substring scan*, or *value list* is only valid for equality and inequality comparisons and means that the field contains any of the values in the list, or the field contains none of the values in the list, respectively.
2. Values can be enclosed in *single, double, or left quotations*. Quotations are **only** required for values that contain a lowercase character, blank, comma, parenthesis, colon, semicolon, a pattern character (% or *) not intended to be the start of a pattern search, or comment character pairs (/* or */).
3. Unquoted strings are converted to uppercase.
4. Quoted strings can suffixed with one of the following *type* characters listed in Table 308. The type determines how the value is to be used.

Table 308. Valid types for quoted string values

Conversion Type	Description
X	Use as a hexadecimal number
B	Use as a bit mask
C	Use as an exact character value

Table 308. Valid types for quoted string values (continued)

Conversion Type	Description
T	Use as a character string in a case-insensitive compare.
G	Use as a pattern in a case-insensitive compare.

5. Quoted character strings that do not specify a *type* and unquoted strings that do not contain any generic symbols are interpreted as type `T`.
6. If the string does not contain any generic symbols or specify any type, it is considered to type `T`.
7. If the string contains generic symbols and is used on a substring scan, it is considered to be type `T`. Otherwise, it is considered type `G`.
8. If a substring scan is used, only types `C` and `T` are supported.
9. If you specify a bit mask value, each bit must be represented by one of the following values: *`0`*, *`1`*, or **`.`** where **`.`** denotes don't care.
10. Conversion to internal format is supported for the following field types.
    - flag (*`YES/NO/ON/OFF`*)
    - binary and hex
    - date
    - access, authority, audit access, audit
    - text

    See "SELECT and EXCLUDE for NEWLIST types other than TYPE=RACF" on page 900 for information about these field types.
11. You can view the type that zSecure assumes for a field by issuing the `SHOW TEMPLATES` command.
12. The formats accepted are like the display format detailed in the "Controlling report and display output for LIST family commands" on page 795, except for the date format. The supported format for date values can be found in "Date fields" on page 903.

segment(*fieldtests***)** *segment*
A number of the *field-value* and *field-field* tests described in "Selection types" on page 885 can be used to select on the following segment names: `CDTINFO`, `CERTDATA`, `CICS`, `DCE`, `DLFDATA`, `DFP`, `EIM`, `KERB`, `LANGUAGE`, `LNOTES`, `NDS`, `NETVIEW`, `OMVS`, `OVM`, `OPERPARM`, `PROXY`, `SESSION`, `SIGVER`, `STDATA`, `SVFMR`, `TME`, `TSO` or `WORKATTR`. The select or exclude criteria must be enclosed in parentheses.The segment name can also be specified by itself to select the specified segment. (See "Examples - SELECT and EXCLUDE statements" on page 908.)

FIELD= *fieldname*
Specifies a field name to be searched for in the profile. Must be used in conjunction with the field name `FIELDVALUE=` or the keyword `SCAN=`, as explained in "Searching by value in a specific field" on page 892 and "Selecting by profile property" on page 889. The field name must be one defined in a template or the word `KEY` to scan the internal profile key (without any class prefix). This parameter is intended for use when the field name is the same as one of the other `SELECT` parameters, or to limit a `SCAN` operation to a specific field.

Selecting by built-in alias names: The following tables lists the built-in alias names that can be used when specifying search criteria.

- "Alias names local to segments" on page 894

- "Alias names for LANGUAGE and SESSION names"
- "Aliases not within a segment"

Alias names local to segments: Table 309 lists the built-in alias names local to segments. These alias names are intended to provide similarity to the RACF commands. These names are only valid in the scope of the corresponding segment selection *segment(...)*.

Table 309. Built-in alias names local to segments

TSO(name())	alias for	OPERPARM(name))	alias for
ACCTNUM	TACCNT	ALTGRP	OPERALTG
DEST	TDEST	AUTH	OPERAUTH
HOLDCLASS	THCLASS	CMDSYS	OPERCMDS
JOBCLASS	TJCLAS	KEY	OPERKEY
MAXSIZE	TMSIZE	LEVEL	OPERLVL
MSGCLASS	TMCLASS	MFORM	OPERMFRM
PROC	TLPROC	MONITOR	OPERMON
SECLABEL	TSOSLABL	MSCOPE	OPERMSCP
SIZE	TLSIZE	ROUTCODE	OPERROUT
SYSOUTCLASS	TSCLASS	STORAGE	OPERSTOR
UNIT	TUNIT		
USERDATA	TUDATA		

Alias names for LANGUAGE and SESSION names: Table 310 lists the built-in alias names that can be used for LANGUAGE and SESSION names.

Table 310. Alias names for LANGUAGE and SESSION

LANGUAGE(*name***())**	alias for	**SESSION(***name***())**	alias for
PRIMARY	USERNL1	INTERVAL	KEYINTVL
PRIM	USERNL1		
SECONDARY	USERNL2		
SEC	USERNL2		

Aliases not within a segment: The following table lists built-in alias names not within a segment.

Table 311. Built-in alias names not within a segment

	alias for
DATA	INSTDATA
UNIT	DEVTYPX
VOL	VOLSER
VOLUME	VOLSER

Selecting profiles by resource class: You can also select and exclude profiles by resource class. The parameters, fields and attributes that can be used for selection criteria depend on the resource class type. See the following topics for details.

- "Fields valid for all resource classes" on page 895

- "Fields valid for the DATASET class" on page 896
- "Fields valid for the USER class" on page 896
- "Fields valid for the GROUP class" on page 899
- "Fields valid for the TAPEVOL class" on page 899

Fields valid for all resource classes: You can use the following parameters and fields to select profiles from any resource class.

CLASS= *class*
CL=*class*
C=*class*
CLASS=(*class***,...)**
The RACF class (USER, GROUP, DATASET, CONNECT, PROGRAM, ACCTNUM, GCICSTRN, ...). The special value GENERAL indicates all kinds of general resource classes. If used with the MATCH or BESTMATCH keywords, the class selection has a special meaning, selecting both a member class and the grouping class. For selection, all normal relational operators and value types, value list and filter specification is supported for example. For more information, see the general "Searching by value in a specific field" on page 892 description.

DISCRETE
Selects discrete profiles.

GENERIC
Selects generic profiles.

HEXKEY= *value*
The profile key in internal, not human-readable format. This value can be used to search for profiles with specific internal values or having specific generic characters.

MEMBERCLASS= *class*
For grouping profiles, this field contains the name of the corresponding member class. For member profiles, this field contains the name of the normal profile class. For all other profile types, this field is undefined.

MEMBERKEY= *key*
For grouping profiles, this repeated field contains the profile keys of all members. For member profiles, this field contains the 'normal' profile key. For all other profile types, this field is undefined.

NOCATEGORY
Select all profiles that do not have a CATEGORY defined.

NODATA
Select all profiles without INSTDATA.

NOSECLABEL
Select all profiles that do not have a SECLABEL defined.

NOSECLEVEL
Select all profiles that do not have a SECLEVEL defined.

NOWARNING
NOWARN
Selects profiles with the warning indicator off.

QUAL= *id*
Q=*id*
The QUAL field matches the first qualifier for data set and general resource profiles, and contains the profile key for user and group profiles. For data set

profiles, *id* matches the first qualifier as changed by ICHCNX00. For selection, all normal relational operators and value types can be used, see the general *fieldname* description.

WARNING
WARN
Selects profiles with the warning indicator on.

Fields valid for the DATASET class: You can use the following attributes to select profiles from the DATASET class.

PADS
Selects DATASET profiles with a non-empty conditional access list as well as profiles in the PROGRAM class.

VSAM
Select DATASET profiles with the VSAM indicator.

NONVSAM
Select non-VSAM data set profiles.

MODEL
Select DATASET profiles with the MODEL indicator on.

NOMODEL
Select DATASET profiles with the MODEL indicator off.

TAPEDSN
Select DATASET profiles with DSTYPE=TAPE.

NOTAPEDSN
NOTAPE
Select DATASET profiles without DSTYPE=TAPE.

GROUPDS
GROUPDSN
Select DATASET profiles with group-data set indicator on.

USERDS
USERDSN
Select DATASET profiles with the user-data set indicator on.

ERASE
Select DATASET profiles with the erase-on-scratch flag on. This is independent of the global ERASE setting.

NOERASE
Select (data set) profiles with the erase-on-scratch flag off. This is independent of the global ERASE setting.

Fields valid for the USER class: You can use the following attributes to select profiles in the USER class.

UAUDIT
Select user profiles that have user-level auditing active.

NOUAUDIT
Select user profiles that have no user-level auditing active.

PASSWORD
Select user profiles that have a password.

NOPASSWORD
Select user profiles that do not have a password.

OIDCARD
OID
Select user profiles that have an OID card key.

NOOIDCARD
NOOID
Select user profiles that do not have an OID card key.

GRPSPEC
GROUPSPECIAL
GROUPSPEC
GROUPSP
GRPSP
GRPSPECIAL
Select USER profiles that contain a group-special connect.

NOGRPSPEC
NOGROUPSPECIAL
NOGROUPSPEC
NOGROUPSP
NOGRPSP
NOGRPSPECIAL
Select USER profiles that contain one or more connect entries without group-SPECIAL. To select a profile without *any* group-SPECIAL connect, use NOT(GRPSPEC).

GRPOPER
GROUPOPERATIONS
GROUPOPER
GROUPOP
GRPOP
GRPOPERATIONS
Select USER profiles that contain a group-OPERATIONS connect.

NOGRPOPER
NOGROUPOPERATIONS
NOGROUPOPER
NOGRPOP
NOGROUPOP
NOGRPOPERATIONS
Select USER profiles that contain one or more connect entries without group-OPERATIONS. To select a profile without *any* group-OPERATIONS connect, use NOT(GRPOPER).

GRPAUD
GROUPAUDITOR
GROUPAUDIT
GROUPAUD
GRPAUDITOR, GRPAUDIT
Select USER profiles that contain a group-AUDITOR connect.

NOGRPAUD
NOGROUPAUDITOR
NOGROUPAUDIT
NOGROUPAUD
NOGRPAUDITOR, NOGRPAUDIT
Select USER profiles that contain one or more connect entries without group-AUDITOR. To select a profile without *any* group-AUDITOR connect, use NOT(GRPAUD).

GRPGRPACC
GROUPGRPACC
Select USER profiles that contain a connect with the GRPACC attribute.

NOGRPGRPACC
NOGROUPGRPACC
Select USER profiles that contain a connect with the NOGRPACC attribute.

GRPREVOKE
GROUPREVOKE
Select profiles that contain a connect with the REVOKE attribute or that were revoked by date and not yet resumed at the day the RACF unload was made (the DUMPDATE). This selects USER profiles with at least one revoked connect.

NOGRPREVOKE
NOGROUPREVOKE
Select profiles that contain a connect without the REVOKE attribute and not yet revoked by date or where the day the RACF unload was made is past the resume date. This selects USER profiles with at least one non-revoked connect.

GRPADSP
GROUPADSP
Select USER profiles that contain a connect with the ADSP attribute.

NOGRPADSP
NOGROUPADSP
Select USER profiles that contain a connect without the ADSP attribute.

NOCLAUTH
Select all USER profiles that do not have any CLAUTH authority.

PWHASHED
HASHEDPW
Select all USER profiles that have a password that is hashed, not encrypted.

PROTECTED
Select all USER profiles that have the PROTECTED (no password, and cannot be logged on with) attribute.

NOPROTECTED
Select all USER profiles that do not have the PROTECTED attribute.

RESTRICTED
Select all USER profiles that have the RESTRICTED (are not granted access through UACC, ID(*) or GAT) attribute.

NORESTRICTED
Select all USER profiles that do not have the RESTRICTED attribute.

SPECIAL
SPEC
Select profiles with the SPECIAL attribute.

NOSPECIAL
NOSPEC
Select profiles without the SPECIAL attribute.

OPERATIONS
OPER
Select profiles with the OPERATIONS attribute.

NOOPERATIONS
NOOPER
Select profiles without the OPERATIONS attribute.

AUDITOR
Select profiles with the AUDITOR attribute.

NOAUDITOR
Select profiles without the AUDITOR attribute.

REVOKE
REVOKED
Select profiles with REVOKE attribute. In addition, the date of the RACF data set unload is used to select profiles that are revoked by date based on the revoke date and resume date fields.

NOREVOKE
NONREVOKED
NOTREVOKED
Select profiles without the REVOKE attribute. In addition, the date of the RACF data set unload is used to verify that profiles are not revoked by date based on the revoke date and resume date fields.

ADSP
Select profiles with the ADSP (automatic data set protection) attribute.

NOADSP
Select profiles with the NOADSP attribute.

GRPACC
Select profiles with the GRPACC (group access) attribute.

NOGRPACC
Select profiles without the GRPACC attribute.

Fields valid for the GROUP class: You can use the following attributes to select profiles in the GROUP class.

NOTERMUACC
NOTERMUACC
Select profiles with the NOTERMUACC (no terminal access based on UACC) attribute.

TERMUACC
Select profiles without the NOTERMUACC attribute.

NOUNIVERSAL
Select profiles with the NOUNIVERSAL (limited amount of connects) attribute.

UNIVERSAL
Select profiles with the UNIVERSAL (unlimited amount of default connects) attribute.

Fields valid for the TAPEVOL class: You can use the following attributes to select profiles in the TAPEVOL class.

SINGLEDS
Selects (tape volume) profiles with the single-data set indicator on.

NOSINGLEDS
Selects (tape volume) profiles with the single-data set indicator off.

AUTOTAPE
AUTO
Select automatic TAPEVOL profiles.

NOAUTOTAPE
NOAUTO
NONAUTO
NOTAUTO
NONAUTOTAPE
NOTAUTOTAPE
Select non-automatic TAPEVOL profiles.

TVTOC
Select TAPEVOL profiles with a TVTOC.

NOTVTOC
Select TAPEVOL profiles without a TVTOC.

SELECT and EXCLUDE for NEWLIST types other than TYPE=RACF

This section describes standard fields that can be used to specify search criteria on SELECT and EXCLUDE statements for NEWLIST types other than TYPE=RACF. These fields can also be used for the NEWLIST subselections specified with the DEFINE command.

For information about the specific fields that can be used with each NEWLIST type, see Chapter 13, "SELECT/LIST Fields," on page 953. For information about selection and exclusion fields for RACF profiles (NEWLIST TYPE=RACF), see "SELECT and EXCLUDE for NEWLIST TYPE=RACF" on page 889.

The field types available with these NEWLIST types and with subselection can be separated into 8 different types, each treated differently.

Table 312. SELECT and EXCLUDE field types for NEWLIST types other than TYPE=RACF

Selection field type	Description
"Character fields" on page 901	These support pattern searches, substring selection, and string conversions.
"Numerical fields" on page 902 (Decimal and hexadecimal)	These fields support numerical conversions.
"Bitfields/Boolean values" on page 902	These fields support ON/OFF or YES/NO selection, as well as specification of bit masks.
"Date fields" on page 903	These fields support dates entered in ISO-format (e.g. 2002-02-02), European format (e.g. 02Feb2002), Julian date format (e.g. 2002/274), TODAY, and NEVER.
"Time fields" on page 904	
"Combined date and time fields" on page 904	Combine any valid date and time format. Enclose each parameter specification in quotations. Separate time and date values with a space.
"Access levels" on page 905	These fields support selection of a single access level or a list of access levels, as well as access higher or lower than the level specified.
Group authority level fields (See "Access levels" on page 905.)	These fields support selection of a single group authority or a list of group authority levels, as well as authority higher or lower than the level specified.
"Matching masks" on page 905	The special keyword MATCH can be used to match a mask field with a specific value.
"UNIX fields" on page 905	These fields allow selection based on file attributes, extended attributes and audit flag settings.

Table 312. SELECT and EXCLUDE field types for NEWLIST types other than TYPE=RACF (continued)

Selection field type	Description
"IPv6 addresses" on page 907	Lists the syntax and rules for selection based on IPv6 addresses.
Instruction-scan fields	These are documented with the NEWLIST type in which the fields are defined. For information about these fields, see Chapter 13, "SELECT/LIST Fields," on page 953.
Other (special format) fields	Typically, these fields cannot be used for SELECT and EXCLUDE processing. They are used only to format output. Exceptions to this rule are documented in "Controlling report and display output for LIST family commands" on page 795. Typically, these fields are of a non-standard format, a time zone field for example.

The following sections describe the different field types listed in Table 312 on page 900. For more information, see "Examples - SELECT and EXCLUDE statements" on page 908.

Character fields: Character fields can be used for `SELECT` and `EXCLUDE` processing in the following ways.

- **Normal string searches** for strings that do not contain wild card characters. These strings are not considered case-sensitive. When a single value is specified, all relational operators are supported. When multiple values are used, only the `=`, `<>`, and `¬=` relational operators are supported. The following example shows a valid search string.

  ```
  select system>SYS1
  select system=(sys1, sys3)
  ```

- **Pattern string searches** for strings containing the following wild card characters: `%`, `*` and `**` or `*` and `-`, with `MASKTYPE=ACF2` . These strings are always converted to uppercase. A list of patterns strings can also be specified. Only the `=`, `<>`, and `¬=` relational operators are supported in pattern string searches.

  ```
  select system<>s%s%
  select system=sys*
  select system<>(sys*, mls*)
  ```

- **Substring searches**. You can select one substring or a list of substrings by specifying a colon (:) after the relational operator. As an alternative, any search string in a list can be prefixed by a colon to indicate a substring search that can include exact matches, substring searches, and pattern matches in a single list. Only the `=`, `<>`, and `¬=` relational operators are supported in pattern string searches.

  If a CARLa `LANGUAGE` statement is specified with the `DBCS` option, the substring scan uses a DBCS-enabled scan function. When this option is active, non-DBCS search arguments are *not* found in DBCS sections of the string, while DBCS search arguments are *only* found in the DBCS sections. See

  Note: The search results are unpredictable if the string has any invalid DBCS section–binary data that has a stray X'0E') for example.

  The following example shows the syntax for searching the system field for occurrences of the substrings `ml` and `sys`.

  ```
  select system=:(ml, sys)
  ```

Strings enclosed in single, double, or left quotations are not used as a pattern. This allows a search for a string or substring containing wild card characters, for instance a specific generic profile. These strings are treated as if they are not

case-sensitive unless appended by the conversion character **C**. Quoted, double-quoted and left-quoted strings can be appended by one of the following conversion characters:

G Treat quoted string as a generic.

X Convert string from hexadecimal (1 to 512 characters).

C Case sensitive string.

T Text string, not case sensitive.

Bitfields/Boolean values: Bitfields and Boolean values are typically used for truth or on/off values. In Security zSecure, truth/on values contain the value X'80'; all other values are false/off. The following selection types are supported.

- The field name alone indicates value is true.
- field=ON, field=YES indicates value is true.
- field=OFF, field=NO indicates value is not true.
- A quoted, double-quoted, or left-quoted value indicates a *bitmask*. This is a binary number with 0 for must-match 0, 1 for must-match 1, and dot (.) for don't care. One to eight bits can be specified; values shorter than 8 bits are padded with don't cares on the left.

The following examples indicate the valid usage.

```
* Select mlstable is TRUE */
select mlstable
select mlstable=yes
select mlstable=on

/* Select mlstable is FALSE */
select mlstable=no
select mlstable=off

/* Bitfield testing the most significant bit only */
select mlstable='1.......'

/* Bitfield testing the least significant bit only */
select mlstable='1'
```

Numerical fields: All numerical fields are treated as values of up to 4 bytes. When one value is specified, all relational operators can be used. When a list of values is specified, only the =, <>, and ¬= relational operators can be used. Any one value can be quoted or double-quoted, with the conversion characters F, X, and B.

F - treat as decimal.

X - treat as hexadecimal, which means that the length is one to eight character and the value is in the set {*0..9,A...F*}.

B - treat as binary, which means that the values *1* and *0*are supported.

The following example shows a valid usage.

```
select profcnt>5
select profcnt=(5,7,13)
select profcnt<>'ff'x
select profcnt='100'b
```

Instead of defining numerical values using digits, you can use the SYMBOLIC statement (`SYMBOLIC NUM name=value`) to define a symbolic name for a numeric value. The symbolic name can be used on its own or associated with a numeric default value that is used if the symbolic has not been defined. The default value is specified as `name|value`.

In the CARLa command input, the symbolic name must be defined before its first use. If you use the conditional specification, the value is the default that is used only if the SYMBOLIC statement has not been defined.

The following code sample defines the symbolic name `maxprof` with a value of `50` and a default value of `100`.

```
symbolic num maxprof=50
select profcnt>maxprof
select profcnt>maxprof|100
```

In this example, the value of `maxprof` in the first SELECT statement is interpreted as `profcnt > 50` as defined by the preceding SYMBOLIC statement. In the second SELECT statement, the select criteria is also interpreted as `profcnt > 50` because the value of `maxprof` is still taken from the SYMBOLIC statement. The select criteria would only use the default value `100` for `maxprof` if the SYMBOLIC statement was not present.

For more information, see “SYMBOLIC” on page 940.

Date fields: The following date formats are supported on input.

Julian date	ISO date	European format
YYDDD YYYY/DDD	YYYY/MM/DD YYYY-MM-DD 'YYYY MM DD'	DDMMMYY DDMMMYYYY DD/MMM/YY DD/MMM/YYYY DD-MMM-YY DD-MMM-YYYY 'DD MMM YY' 'DD MMM YYYY'

2-digit years are generally considered an error. However, you can suppress the error message by means of the SUPPRESS MSG= (51,53) command. In that case, 2-digit years are interpreted as prefixed with 19.

You do not have to specify leading zeros for the month and day of the month, e.g. 2001/2/3 is an acceptable input format for February 3, 2001.

In addition to the normal dates, zSecure Admin and Audit supports three special values.

Special values	Explanation
DUMPDATE	The date that the UNLOAD you have connected was created, or if you have connected the active security database, today.
NEVER	The date field has never been set, or has been reset to its initial state. E.g., PASSDATE=NEVER looks for users who have never changed their password. NEVER is only useful when using the = or <> operators.
TODAY	Today.

The special values can be followed by a displacement in days, either + or - followed by a decimal number, for example TODAY-30 , or a displacement keyword. Do not enter blanks before the displacement value. Note that not all date fields support DUMPDATE. For example, the certificate fields CERTSTRT and CERTEND do not allow this special value.

The following (RACF) keywords can be used as displacement keyword.

Displacement keyword	Explanation
INACTIVE	The number of days before inactive user IDs will be revoked
INTERVAL	The maximum number of days before a password change is required by a user.
SESSINTV	The maximum number of days before a session key expires

Date formats using blanks as separators must be surrounded by single quotes, double quotes, or left quotations. For selecting, a range of dates separated by a colon (:) is also supported, as indicated in the following examples.

```
SELECT DATE=01JAN1994                    /* One date */
SELECT DATE=(31DEC1993, 27SEP1994)       /* Two dates */
SELECT DATE>=01JAN1994 DATE<=31DEC1996   /* Date range */
SELECT DATE=01JAN1994:31DEC1996          /* Date range */
```

Time fields: For SELECT/EXCLUDE processing, values in the range 0000 to 2359 are supported. The default output size is five characters long (18:00 for six o'clock PM); use an overriding length of 8 to get seconds, and an overriding length of 11 to get 1/100 seconds. The time selection format 'HHMM' can be produced by a preceding CARLa run if you use overriding length 4 on a field in SMFTIME (for binary 4-byte fields such as this one) or TIME (for unsigned packed decimal fields as can for example be found in RACF profiles).

For SELECT/EXCLUDE processing, a range of times separated by a colon (:) is supported, as indicated in the following examples.

```
SELECT TIME=0800                          /* One minute */
SELECT TIME>=0900 TIME<=1600              /* Time range */
SELECT TIME=0900:1600                     /* Time range */
```

When specifying a time for SELECT/EXCLUDE processing, the time value is rounded to minutes before comparison. For example TIME<1745 selects any time up to 17:44:59.99, and excludes any time from 17:45:00.00, and TIME<=1745 selects any time up to 17:45.59.99, and excludes any time from 17:46:00.00.

Combined date and time fields: For SELECT and EXCLUDE processing any date format as specified in the preceding paragraphs is supported. If a time is also to be specified, it should be specified as `[h]h:mm:ss.cc`. You can leave out the centiseconds, the seconds or the minutes and seconds. These missing parts are rounded either up or down, depending on the logic of the select statement. Time and date should be separated by a space, and quoted. A range of combined dates and times separated by a colon (:) is supported.

The following examples indicate a cross-section of the valid usages.

```
SELECT DATETIME=23Sep2002            /*one day*/
SELECT DATETIME='23Sep2002 08:30'    /*one minute*/
SELECT DATETIME=23Sep2002:25/Sep/2002
                                     /*range of three days*/
SELECT DATETIME='23Sep2002 8:30:00.00':'23Sep2002 8:30:30'
                                     /*range of thirty seconds*/
SELECT DATETIME>'23Sep2002 22'       /*after ten o'clock*/
SELECT DATETIME<'23-Sep-2002 17:45'  /*up to 17:44:59.99*/
SELECT DATETIME<='23-Sep-2002 17:45' /*up to 17:45:59.99*/
```

Access levels: Selection of fields containing RACF access levels can be one of the following.

- Selection of a single value, for example FIELD=*level*. The relational operators =, <>, ¬=, <, >, <=, and >= can be used.
- Selection of any of a list of access levels, for example FIELD=(*level1*,*level2*,...). The relational operators =, <>, and ¬= can be used.

The following access levels are supported; listed in increasing sort order.

```
NONE
EXECUTE
READ
UPDATE
CONTROL
ALTER
```

The following examples show a valid usage.

```
/* Select access level of UPDATE or higher */
select access>=update

/* Select any access level but CONTROL and EXECUTE */
select access<>(control,execute)
```

Matching masks: The special keyword MATCH can be used to match a mask field with a specific value. This keyword is governed by the following syntax: MATCH[=](*field=value*). This specification selects those field values that cover the specified value. The field is treated as a mask of the appropriate type, EGN or NOEGN for example. The specified value cannot contain wild cards.

As an example, the following statement selects RACF access records (permits and member list entries used for RACF access checking) describing GCICSTRN class profiles that contain the value CEMT in the profile key or with a generic that matches the value CEMT. It prints the value(s) from the profile member list along with the access list.

```
newlist type=racf_access title="Access matching CEMT transaction"
  select class=gcicstrn match=(member_key=cemt)
  sortlist member_key profile id access
```

The MATCH keyword and syntax are valid for all NEWLIST types other than NEWLIST TYPE=RACF. However, most NEWLIST types do not have any fields that can contain masked values. Using MATCH for fields that cannot be masks can yield unpredictable results.

UNIX fields: For the file attributes, extended attributes and audit flag settings, it is possible to use the standard output format for equality selection (and for file attributes OCTAL is supported as well). However, it is possible to select on the

presence or absence of some separate attributes or settings as well using an extended syntax. Use of this extended syntax is signalled by quoting the specification and appending an 'M'.

File attributes: For file attributes, this syntax is an extension of the CHMOD output format. See “File attributes” on page 825). You can select on the attributes of one or two groups instead of all of them. You can also select on the presence or absence of separate bits rather than the entire group by using + (on) and - (off) instead of =. If you include multiple clauses, separate clauses with commas. Clauses are processed with AND logic. If the clauses contradict each other a syntax error is issued.

For example, you can specify the following selection statement to identify all files that have a SETUID property that is world-executable.

```
SELECT ATTR='u+s,o+x'M
```

Alternatively, the u, g, and o indications can be omitted entirely. In that case, the access indicated results in a match if a match exists for **any** of these groups. That is, OR logic is implied.

If an indication only applies to u and g(s) or o(t), it only matches for those groups (so *+t*M is equivalent to *o+tM*). This type of specification (referred to as *nonspecific*) cannot be combined with u, g, or o' specific clauses within the same mask.

The ATTR syntax also applies to the UNIX_ACCESS_ALLOWED and UNIX_ACCESS_USED fields of SMF NEWLIST. For these fields 'u', 'g' or 'o' specific clauses are evaluated by looking at the corresponding UNIX_ACCESS_ORIGIN field. For 'u' it should be 'user', for 'g' it should be 'group' and for 'o' it should be 'other'. Note that 'u' will **not** match with UNIX_ACCESS_ORIGIN='user ACL'. If UNIX_ACCESS_ORIGIN contains any value other than these three, only the "nonspecific" type of specification might match. In general the "nonspecific" type is the best option for the TYPE=SMF fields.

For example,

```
SELECT UNIX_ACCESS_USED='+w'M UNIX_ACCESS_ORIGIN=('user'c,'user ACL'c)
```

will select records where write access was used that was granted to a specific user (either through the owner bits, or through an ACL entry).

"Nonspecific" specification is also supported without the use of a mask (e.g., SELECT UNIX_ACCESS_ALLOWED=r--).

Extended attributes: For the extended attributes, this syntax is a similar extension of the EXTATTR output format (see “Extended attributes” on page 826).

For example,

```
SELECT EXTATTR='-s'M
```

selects those file that ignore the _BPX_SHAREAS setting and on execution of the file start a new address space anyway.

The following statement selects files without APF authorization, with program control, and with the share-AS attribute.

```
SELECT EXTATTR=-ps
```

The following statement, selects files without program control, and without the share-AS attribute.

```
SELECT  EXTATTR='-ps'M
```

Audit flags: For the audit flags, this syntax is a similar extension of the CHAUDIT output format. See “Audit flags” on page 826). (Note that the "nonspecific" alternative specification type is not supported here.)

For example,

```
SELECT AUDITFLAGS_AUDITOR='x+sf'M
```

selects those files for which the auditor has requested both success and failure auditing for execute access.

Note: The "nonspecific" alternative specification type is not supported here.

IPv6 addresses: Selection of an IPv6 address is supported only if the address is enclosed in quotes and adheres to the following rules.

- The IPv6 address value does not have any leading zeros in front of any block of 1 to 4 hexadecimal digits.

  Examples

  – **Supported address value:** 9::ABC

  – **Unsupported address value:**

  `09::ABC` has a leading *0* in front of *9*.

  `9::0ABC` has a leading *0* in front of *ABC*.
- For IPv6 address values, the rightmost largest sequence of *0* blocks (`0 : 0 : 0 : ... : 0`), including

  Examples

  – **Supported address values:**

  `1234:0:0:DEF0:1234::DEF0`

  `1234::1234:0:0:DEF0`

  `1234:5678:1234:5678:1234:5678::5678`

  – **Unsupported address value:**

  `1234::DEF0:1234:0:0:DEF0` has its leftmost rather than its rightmost largest sequence of *0* blocks abbreviated with `::`.

  `1234:0:0:0:1234::DEF0` has an abbreviation `::` that stands for a sequence of two *0* blocks, but the address has a larger sequence of *0* blocks.

  `1234:5678:1234:5678:1234:5678:0:5678` does not have its largest sequence of *0* blocks (consisting of a single 0 block) abbreviated with `::`.
- The address does not contain a *0* block right before or right after a `::`.

  Examples

  – **Supported address value:** `::` and `6789::FFFF`

  – **Unsupported address value:**

  `0::0` has a *0* block right before as well as a *0* block right after the `::`.

  `6789::0:FFFF` has a *0* block right after the `::`.

  `6789:0::FFFF` has a *0* block right before the `::`.
- For IPv4-mapped IPv6 addresses–addresses with 26 bytes *0* followed by 2 bytes *FF* followed by 4 other bytes, then its rightmost 4 bytes are written as an IPv4 address without any leading zeros.

Examples

– **Supported address value**: `::FFFF:1.2.3.4`

– **Unsupported address values**

`::FFFF:102:304` is not supported because it does not have its rightmost 4 bytes written as an IPv4 address.

`::FFFF:1.2.3.04` is not supported because the address has a leading *0* in front of the *4*.

- If the address is not an IPv4-mapped IPv6 address, then its last 4 bytes are not written as an IPv4 address.

  Examples

  Supported address values: `::102:304` and `9876::5432:102:304`

  Unsupported address values:

  `::1.2.3.4` is not supported because it is not an IPv4-mapped IPv6 address, but its last 4 bytes are written as an IPv4 address.

  `9876::5432:1.2.3.4` is not supported because it is not an IPv4-mapped IPv6 address but its last 4 bytes are written as an IPv4 address.

Examples - SELECT and EXCLUDE statements

Table 313 provides examples showing different criteria and tests that can be used to select and exclude records.

Table 313. Example for SELECT and EXCLUDE statement

Selection criteria	Example
Implicit AND function	This example selects data set profiles with a first qualifier of SYS1. It illustrates the AND function between the parameters on one SELECT statement. `select class=dataset qual=sys1`

Implicit OR function	This example selects data set profiles as well as DLFDATA profiles that match a filter SYS1.** (for example, everything with SYS1 as the first qualifier). It illustrates the OR function between multiple SELECT statements.
	`select class=dataset filter=sys1.**`
	`select class=dlfdata filter=sys1.**`

Explicit AND and OR function	This example selects data set profiles as well as DLFDATA profiles that match the filter `SYS1.**`–all profiles with *SYS1* as the first qualifier. It illustrates the explicit AND and OR functions and the use of parentheses.
	`select ((class=dataset or class=dlfdata) and filter=sys1.**)`
	As an alternative, a list of values could have been used.
	`select class=(dataset,dlfdata) filter=sys1.**`

Combining select and exclude	This example selects data set profiles with UACC greater than NONE, but excludes all SYS2 profiles. This illustrates the exception function of the EXCLUDE command.
	`select class=dataset uacc>none`
	`exclude filter=sys2.**`

Table 313. Example for SELECT and EXCLUDE statement (continued)

Selection criteria	Example
Multiple keywords	This example illustrates the multiple scan facility. It is much more efficient than repeated SELECT commands that would produce the same result. `select scan=('JONES',parker,'SMITH',perry)` **Note:** The SCAN= operand value is always converted to uppercase unless it is enclosed in quotations.
Segment field value selection	This example illustrates the use of the segment field selection mimicking TSO syntax. `select dfp(mgmtclas(fastmig))`
Field value filter	This example illustrates the use of a generic character in the field selection. The selection selects all profiles that have an owner field starting with 'SYS'. `select owner=sys*`
Field value scan	This example illustrates the use of the scan character in the field selection. The selection selects all user profile base segments that have a name containing JONES in an arbitrary position in the field. `select c=user s=base name=:JONES`
Class name filter	This example illustrates the use of a generic character in the class name. The command selects all base segments in the CICS transaction classes. `select c=%CICSTRN s=base`

MATCH	In this example, the command lists all profiles that could protect the data set specified using the MATCH keyword. The SEARCHKEY output field is used to sort on *best match*. If more specific profiles are deleted, the less specific profiles are used to protect the data set. (The less specific profiles are listed before the more specific profiles.)
	`newlist`
	`select class=dataset match=CKR.SCKRLOAD`
	`sortlist class searchkey(nondisplay) key proftype uacc`
	
	Note: If discrete profiles are listed, the data set is only protected by that profile if the indicated bit is set and the volume serials match. If these do not match, the most specific generic profile is used.

MATCH for grouping and member classes	The MATCH keyword matches both member profiles and the member list of grouping profiles. When the CLASS keyword is also used and specifies a member class, the grouping class is automatically included. The following example displays all profiles that could protect a CICS transaction.
	`newlist`
	`select class=tcicstrn match=prodcics.cemt`
	`sortlist class key memlst / acl(header)`
	
	If both CLASS and MATCH are specified, these keywords *must* be specified as the first keywords of a SELECT/EXCLUDE clause or WHERE clause.

Table 313. Example for SELECT and EXCLUDE statement (continued)

Selection criteria	Example

ACL repeat group combination (access list entries)	The following example uses the ACL(...) keyword to select the profiles where any defined user that is not RESTRICTED has unconditional access higher than READ. For each profile the UACC and the unconditional access of ID(*) are printed in separate columns.
	`newlist title="Unspecific access of update or more"`
	`  select ACL(id='*' missing(whenprof) access>READ) or,`
	`  (not(ACL(id='*' missing(whenprof))) uacc>READ)`
	`  define definedacc("ID(*)",aclaccess) subselect,`
	`  ACL(id='*' missing(whenprof))`
	`  sortlist class key uacc definedacc`

USR repeat group combination (userdata entries)	This example illustrates the use of the USR(...) keyword. The following example displays the profiles where the userdata field PHONE contains a number starting with area code 555 (assuming the installation defined such userdata fields) with any phone numbers included in them.
	`newlist`
	`  select usr(usrnm=phone usrdata=555*)`
	`  def phone subselect usr(usrnm=phone)`
	`  sortlist class key phone`

Custom field	This example selects all users in finance and shows the NAME fields and all custom fields.
	`newlist type=racf`
	`select class=user segment=csdata`
	`custom_data(cskey=dept csvalue='finance')`
	`sortlist key(8) name custom_data`
	An alternative way of making the selection without showing the field list header as a prefix is shown in the following example.
	`newlist type=racf`
	`select class=user segment=csdata dept='finance'`
	`sortlist key(8) name dept`

SHOW

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command can be used to request fixed-format reports where the sort order cannot be changed, unlike reports requested with the REPORT option, or NEWLISTs with a user-defined layout.

CKRSITE
List the installation-defined settings stored in the CKRSITE module on the SYSPRINT file. The CKRSITE module and its contents are described in *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. This command issues message CKR0525.

CLASSES
CLASS
List the number of generic and discrete profiles for each resource class, as well as the number of segments per entity type. This option is not supported in restricted mode. This includes CARLa script CKRLCLAS.

ICHNCV00
Show the RACF naming convention table ICHNCV00 in assembler format on the SYSPRINT file. This issues message CKR0594.

TEMPLATES
TEMPLATE
List all fields present in the templates, together with the default input and output format assigned by Security zSecure, and a description of the main application of the field. The sort order is by field name. Sample output is present in Chapter 3, "RACF Audit Guide," on page 255. This includes CARLa script CKRLTEMP.

ZAP
This is an alias of CKRSITE.

Example - show templates

The following command requests a listing of all template fields.

```
show templates
```

Sample output is included in "TEMPLATE - Template field properties" on page 284.

Example - show CKRSITE

The following sample output shows a listing of the CKRSITE module with installation-defined settings. Note that the CKGRACF command gives a more complete listing of the CKRSITE module.

```
show ckrsite
CKR0525 00 Contents of CKRSITE module:
           Class:              XFACILIT
           Authority:          SINGLE
           Force restrict:     N
```

This message indicates that the CKGRACF, menu option and action authorization checks are done in class XFACILIT; that the default multiple-authority setting is SINGLE; and finally that Security zSecure is not forced in restricted mode.

Example - show ICHNCV00

The following sample output shows a listing of the RACF naming convention table ICHNCV00. For each system, the date and time is listed that the module was created, followed by reconstructed source code.

```
show ichncv00
CKR0594 00 System 3090: using ICHNCV00 of 01/11/95 17.29
           Can be simulated by Security zSecure
           Reconstructed ICHNCV00 source code follows
CHECK1   ICHNCONV DEFINE,NAME=CHECK1
         ICHNCONV SELECT,COND=((GQ,1),EQ,'SYS1')
         ICHNCONV ACTION,SET=((UQ,0),'RCOPROB')
         ICHNCONV END,NEXT='SUCCESS'
         ICHNCONV FINAL
```

SIMULATE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the SIMULATE command, or its abbreviation SIM, to change a number of settings or to add features globally in the CKRCARLA run. You can use this command to test scenarios without actually making changes in the security database.

SIMULATE commands have several subtypes. The subtype is entered as the first positional parameter on the command.

```
CLASS=class [ACCESS=[level | READ] [SENSITIVITY=Site<text>
PRIO={2|3|4|5|6|7|8|9} [ID=S<id>] CONCERN='concern
text'][[RESOURCE_LOCATION|RESLOC]=name] RESOURCE=(name, ...)
```

Applies to the RESOURCE field in the NEWLIST TYPE=RACF_ACCESS and to data sets and resources in NEWLIST TYPE=TRUSTED. When this option is specified, the program uses resource simulation to show which permit is used for which resource for RACLIST-merged grouping and member profiles. For CLASS=DATASET, this statement adds a sensitive resource and optionally adds resource locations if locations are reported by NEWLIST TYPE=REPORT_*.

For the command syntax, CLASS must be the first parameter and RESOURCE the last parameter. The CONCERN parameter must be specified as the last optional parameter before the RESOURCE parameter. If the CONCERN parameter is specified, the parameters PRIO and SENSITIVITY must also be specified. The RESOURCE parameter can contain a list of resource names separated by commas or blanks. End of line characters between parentheses are ignored. Resource names are case sensitive. The SIMULATE command can be combined with the SUPPRESS AUTO_RESOURCE command so that only the resources specified on SIMULATE commands are included in the output. See the SUPPRESS command.

To influence how many resources get reported, use the REPORT RESOURCE command to automatically include sensitive general resources, or use the REPORT DATASET command to automatically include sensitive data sets, or use the REPORT RESOURCE DATASET command to include both. Before using the REPORT commands, consider how much output you require, especially when including the DATASET option. If you do not specify any additional selection criteria (SELECT command), adding many resources by using the SIMULATE command combined with the use of the RESOURCE field in NEWLIST TYPE=RACF_ACCESS can result in an exceedingly high volume of output. The amount of output generated equals the product of the number of resources in system multiplied by the number of permits in the profiles that protect the resources.

The following classes assign a non-standard meaning to the member list and are not supported for resource simulation: CONNECT, DIGTNMAP, DIGTCERT, DIRACC, DIRAUTH, FSSEC, FSOBJ, GLOBAL, GMBR, GROUP, IDIDMAP, NDSLINK, NODES, NODMBR, NOTELINK, PMBR, PROGRAM, RACFVARS, RVARSMBR, SCDMBR, SECDATA, SECLABEL, SECLMBR, UNIXMAP, USER, VMBR, VMEVENT, VMXEVENT, and VXMBR.

The following definitions of the optional parameters for the SIMULATE command provide descriptions, syntax, and processing considerations.

[ACCESS=[level | READ]
The minimum access level associated with the RISK field. READ is the default.

CONCERN=['text' | "text" | `text`]
Audit concern description that explains the authority granted by the sensitive access level defined in the ACCESS field. The CONCERN parameter is reported in NEWLIST TYPE=TRUSTED. Specify the CONCERN

parameter as the last optional parameter before the RESOURCE parameter. The maximum length is 64 characters. The description text must be enclosed in quotes. If the optional CONCERN parameter is specified, the PRIO and SENSITIVITY parameters must also be specified.

PRIO={2|3|4|5|6|7|8|9}
Audit priority is a number in the range of 2–9 that determines the display sort order of the audit concern. Priority 2 represents the lowest priority. Priority 1 is reserved for inactive userids that have been revoked or suspended. Priority 9 is very high, system-wide systems programmer privilege. The default priority for CICS resources is 2, but the PRIO parameter can be used to increase the CICS audit priority. If the optional PRIO parameter is specified, the CONCERN and SENSITIVITY parameters must also be specified.

SENSITIVITY=Site<text>
An 11-character string that denotes the sensitive resource type. The text string must start with 'Site'. The case of the text string is preserved.

ID=S<id>
The ID=*parm* can be specified on the LANGUAGE statement that specifies the translation. The ID must start with an 'S' and its maximum length is 8 characters. If the optional ID parameter is specified, the CONCERN, PRIO, and SENSITIVITY parameters must also be specified.

RESLOC=<resloc> | RESOURCE_LOCATION=<resloc>
Optional specification of the location of the CLASS RESOURCE. The CLASS_RESOURCE location is returned in various reports in the RESOURCE_LOCATION field. The maximum length is 35 characters. The text is converted to uppercase.

CNGRACF
CNGRACF CLASS=*class*
CNGRACF COMPLEX=*complex*
CNGRACF COMPLEX=*complex* **CLASS=***class*
CKGRACF
CKGRACF CLASS=*class*
CKGRACF COMPLEX=*complex*
CKGRACF COMPLEX=*complex* **CLASS=***class*
These command subtypes can be used to influence the CKGRACF scope determined by the program. SIMULATE CKGRACF causes resources of the form CKG.** to be checked. SIMULATE CNGRACF causes resources of the form $CNG.** to be checked. The two command subtypes are mutually exclusive on the complex level. If the COMPLEX= keyword is used, only the specified complex is affected by the command. If the COMPLEX= keyword is omitted, all complexes that are not the target of a specific SIMULATE CNGRACF or SIMULATE CKGRACF command are affected. A complex that is the target of neither is processed like for SIMULATE CKGRACF, unless it contains an UNLOAD file made by an old version of the product that still used the $CNG.** resources, in which case SIMULATE CNGRACF processing applies. The CLASS= keyword specifies the general resource class to be checked. If omitted, CKG.** resources are checked in the class specified in the CKRSITE module (or XFACILIT if there is none), whereas $CNG.** resources are by default checked in FACILITY. These command subtypes are not supported in restricted mode.

DMSPARMS *prm+val*
This command sub-type can be used to simulate the effect of changing DMS parameter settings, or, if they are missing from the CKFREEZE file, to tell the

program how they are set. The parameter name and value are specified without intervening blanks, as in the DMS option members. The following parameters are supported and used.

RACFALWZ
Always-call must be Y to process data sets that are not RACF-indicated.

RACFBKUP
Determines the way discretes are processed.

RACFPRED
Determines whether an existing discrete will be used or deleted when a data set is restored.

RACFSUPP
Support must be Y to support RACF-indicated data sets.

RACFPROC
Process RACF profiles can be Y to be able to process data sets that have lost their discrete profiles.

RACFNEWN
Process NEWNAME must be N for a safe system.

RACFDVOL
Volume for discretes

RACFUSID
High-level qualifier for archive data sets.

SECURVOL
Determines whether DASDVOL profile are checked first.

POLICY *policy*
This option is only used in the audit products. It sets the policy against which settings are checked. It causes additional audit concerns to be raised. Also, it increases priority for direct violations of the policy to be at least 40. It is by no means a complete check on all requirements for the policy.

The policy can be one of the levels C1, C2, or B1 from the US standard DOD 5200.28-STD, usually called 'orange book'. C2 is equivalent to the Protection Profile CS1 (Commercial Security 1) of the Common Criteria. If no explicit policy is requested, the built-in IBM Security zSecure audit policy will be used, somewhere between C1 and C2 but with more emphasis on auditing.

RACF_ACCESS

This option controls under which profile, profile member, and access list entry the Access Monitor records will be reported in `RACF_ACCESS NEWLIST`.

When `SIMULATE RACF_ACCESS` is **not** specified, the result fields in the Access Monitor records are used to locate the profile name in the current RACF input source and if the profile exists, occurrences are counted towards that profile.

When `SIMULATE RACF_ACCESS` is specified, the result fields of the Access Monitor records are not used, and a simulation is done of what RACF would do given the current RACF input source. The profile resulting from that simulation is used for recording and counting purposes. This option also determines whether the Access Monitor records are counted as success, violation, or unexpected.

Note that specifying the `RACF_ACCESS NEWLIST` option without using the `SIMULATE RACF_ACCESS` option precludes the use of the `SIM*` fields in `RACF_ACCESS NEWLIST`. That is, when you set up a reporting query using both the `RACF_ACCESS` and `ACCESS` NEWLIST types together, you must specify the `SIMULATE RACF_ACCESS` option to include SIM* field data in the report results. If you do not specify this option, the `SIM*` fields will be empty.

RDEF FACILITY IRR.PGMSECURITY APPLDATA(' *mode*')
Simulate that FACILITY profile IRR.PGMSECURITY has APPLDATA('*mode*'). This simulates the mode in which RACF Program Control runs. The following modes are supported.

- BASIC for basic security mode
- ENHWARN for Enhanced-Warning security mode
- ENHANCED for Enhanced security mode

This command is used with VERIFY PADS (see "VERIFY PADS" on page 943). You can evaluate the commands that are generated by VERIFY PADS before configuring RACF in the mode.

RESTRICT
This option causes Security zSecure to behave as if it were called in restricted mode. This can be used before introducing restricted mode to study the effect, or to develop Security zSecure input that has to be usable in PADS mode. There are no further parameters to the command.

SENS *type* **SENSITIVE ...**
This command subtype can be used to add system data sets to be considered integrity sensitive by the REPORT SENSITIVE command and newlists of type REPORT_SENSITIVE, SENSDSN or TRUSTED. The *type* can be:

LINKLIST
non-APF data sets in LNKLSTxx

PROCLIB
JES2/JES3 non-STC/TSU procedure libraries

Access of UPDATE or more will be considered an exposure.

SENS *acc cls name*
SENSITIVE ...
This command subtype can be used to add data sets to be considered by the REPORT SENSITIVE command and NEWLIST types: REPORT_SENSITIVE, SENSDSN, or TRUSTED. For SENSDSN it is only effective for queries that read the entire CKFREEZE file for different reasons (this is not ensured because of this command). The data sets are only processed if they exist; the specification is ignored if a matching data set does not exist. Three additional positional parameters must be given.

acc
gives the access that must be considered an exposure. It must be READ or UPDATE, or abbreviated R or U.

cls
Class name, must be DATASET, D, or DSN.

name
Resource name, fully qualified data set name (without quotations).

SETROPTS *options*
SETR *options*
This allows one to simulate the effect of changing selected system-wide RACF options. The syntax of the rest of the command is similar to the RACF SETROPTS command. The SETROPTS options supported are MODEL, TAPEDSN, PROTECTALL, EGN, ERASE, and WHEN with their respective subparameters and opposites. The SIMULATE SETROPTS command is not supported in restricted mode.

SHARED
SHARE
NONSHARED
NOTSHARED
UNSHARED

NOSHARED
NOSHARE
NONSHARE
NOTSHARE **SYS=***list* **VOL=***list* **SYS=***list* **VOL=***list*

This command subtype can be used to override the default shared DASD layout interpretation (which is based on the UCB settings). The command accepts two optional parameters: SYSTEM (or its aliases SYSTEMS, SYST, and SYS), and VOLUME (or its aliases VOLSER and VOL). Both parameters accept a single value (system name / volume serial), or a list of values enclosed in parentheses and separated by commas. The scope of the SHARED / NONSHARED command is determined by the two parameters. If absent, it applies to all systems and all volumes. If no volume is included, it applies to all volumes in the systems mentioned. If no system is included, it applies to all systems for the volumes mentioned. If multiple commands apply to the same volume and/or system, the order of priority for each system/volume combination is shown in the following list.

1. Sim (non)shared System= Volume=
2. Sim (non)shared Volume=
3. Sim (non)shared System=
4. Sim (non)shared
5. Use Shared setting from UCB.

If the system and volume parameters are both omitted, the command must be terminated by a semicolon.

SMF=*number*
SYSTEM=*smfid*
FORMAT=*fmt*

Interpret the indicated SMF record number as a record of type *fmt*. This specification might be needed if you do not have an appropriate CKFREEZE for the system you want to analyze *fmt* records from. If a CKFREEZE is present, the program should automatically select the proper format. When no *smfid* is specified, the command affects all systems. Otherwise, a CKFREEZE with the *smfid* specified should be present, or the command will be ignored.

When multiple record numbers are specified (maybe one from a CKFREEZE and one from SIMULATE) for one format, all will be interpreted as being of that specific format.

The following formats are supported.

- ACF2
- AIM
- HSM0
- HSM1
- OMEG
- SECURPASS

TODAY=*date*

This parameter can be used to turn out reports as if it were the specified date. The supported format for date values can be found in “Date fields” on page 903.

This is especially useful for regression testing, and answering what-if questions. The main area of impact is output that depends on a comparison of date values with the current date (like revoke status). The datestamp printed on the output will also list the simulated date, except the first (or all) pages in the SYSPRINT

file. Faked time stamps might be recognized when they display the time as well as the date, because the time has been set to the impossible `HH:MM:SS.CC` value *`99:00:00.00`*. The date value can also be used to recognize unloads that have been unloaded with a simulated today value. The parameter is not supported in restricted mode.

Example - Including tape data sets for VERIFY

The following example shows how to include the tape data sets into consideration for VERIFY NONEMPTY.

```
simulate setropts tapedsn
verify nonempty
```

SMFCACHE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•			•	•	•

The SMFCACHE command controls the SMF job tag system. It can be used outside the context of a NEWLIST TYPE=SMF command, and has the following parameters.

ON
Turn the job tag system on (default).

OFF
Turn the job tag system off.

MINIMAL
Turn the job tag system on, but do not delay records.

RECORDS= *number*
Set the overall amount of records that might be delayed.

JOBRECORDS= *number*
Set the per-job tag amount of records that might be delayed.

VERBOSE
Print job tag statistics during run.

The RECORDS parameter sets the number of records that might be delayed for all incomplete job tags combined, while the JOBRECORDS sets the number of records that might be delayed for any one incomplete job tag. The value of RECORDS should be larger than the number of multi-user address spaces multiplied by the value of JOBRECORDS. Default values are 2000 (RECORDS) and 100 (JOBRECORDS).

The MINIMAL parameter turns on the job tag system and sets the value of RECORDS to zero. This means that records are never delayed, but any record with a complete job tag can still be completed. Use the MINIMAL parameter when memory is tight, or when you are processing SMF data on TSO.

The VERBOSE parameter causes Security zSecure to print a statistic message each time a job tag with cached records is completed and each time a tag cannot be completed as well as a message detailing memory usage statistics at the end of SMF processing. These messages can help determine the proper SMFCACHE settings and SMF interval time at your installation. The messages codes are

CKR0455, CKR0456 and CKR0457. Additional information about these messages is available in the *IBM Security zSecure: Messages Guide*.

SORTLIST

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

This command has the same syntax as the LIST command. It is followed by a list of field names. However, unlike the LIST command, the SORTLIST command lists records in ascending sequence of the fields to be listed. If you specify the class and key fields as shown in the following example, the class and profile key of the selected records are output sorted in ascending sequence.

```
sortlist class key
```

Another difference is that in the scope of a NEWLIST command, the SORTLIST generates page and column headers by default, while the LIST command does *not* generate any page and column headers by default.

However, the sort order is based on the *internal representation* of the fields. This might become apparent when the field is formatted by a format. Different internal values might result in the same output string (for instance, with a date format both the null and the undefined values format as blanks, while they are at the opposite end of the sort spectrum).

To change the sort order from the default *column order* to another order, add the sort keys in front with the NONDISPL attribute.

For fields that are part of a *repeat group*, the position of the record in the output is based on the value of the first occurrence of the field in the repeat group (this is the value listed in the first output line for the profile). The order of the repeat group entries themselves is not sorted, but the same as it appears in the input source. For example, a command SORTLIST user ID KEY would sort based on the first user ID in the access list.

To remove duplicate entries from a SORTLIST, use the NEWLIST NODUP parameter.

For a further discussion of the syntax as well as examples, see the reference section on LIST.

SUMMARY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the SUMMARY command or its variant DSUMMARY for listing data in ISPF panels, to create summary reports of selected data. The summary reports can also contain the selected data itself.

The basic features of the SUMMARY command are explained in an extended example in the "Basic Concepts" followed by more detailed information. More detailed information is available in the remaining topics.

Basic concepts

The following extended example illustrates basic concepts for using the SUMMARY command. The data in the example is not based on real-world information.

Table 314 represents data from eight records that comes from the following fields: CLASS, OWNER, QUAL, and KEY fields. This CARLa statement to produce this report is: SORTLIST CLASS OWNER QUAL KEY

Table 314. Record data - CLASS, OWNER, QUAL, and KEY data for eight records

Class	Owner	Qual	Key
DATASET	ONE	SYS1	SYS1.ONE.AA
DATASET	ONE	SYS2	SYS2.ONE.AA
DATASET	ONE	SYS2	SYS2.ONE.BB
DATASET	TWO	SYS1	SYS1.TWO.AA
DATASET	TWO	SYS1	SYS1.TWO.BB
DATASET	TWO	SYS2	SYS2.TWO.AA
DATASET	TWO	SYS2	SYS2.TWO.BB
DATASET	TWO	SYS2	SYS2.TWO.CC

CARLa command statement: SORTLIST CLASS OWNER QUAL KEY

You can create sorted output like that shown in "Using the summary statement - examples" on page 927 using the SORTLIST and DISPLAY commands.

Using the data shown in "Using the summary statement - examples" on page 927, you can use a SUMMARY command to create an overview that only shows the QUAL field data for each CLASS, OWNER combination. This summary can be created using a two-level summary: Summarize the information for each CLASS and OWNER combination and include only the information from the QUAL field. The CARLa statement to produce this report is: SUMMARY CLASS OWNER * qual.

Table 315 on page 920 shows the results of the two-level summary using the example data.

Table 315. Two-level SUMMARY report - QUAL field data summarized by CLASS and OWNER for eight records

Class	Owner	Qual	Count
DATASET	ONE		3
		SYS1	1
		SYS2	2
DATASET	TWO		5
		SYS1	2
		SYS2	3

CARLa command statement: SUMMARY CLASS OWNER * qual

In this summary, you see the following results:

- The CLASS, OWNER combination DATASET ONE occurs three times.
- The CLASS, OWNER combination DATASET TWO occurs five times.
- The combination DATASET TWO, QUAL SYS1 occurs two times.
- The combination DATASET TWO, QUAL SYS2 occurs three times.

The summary does not include the full data. In this example, the data from the KEY field is not listed. You can create a summary like this using only the SUMMARY command. The **Count** field is an example of a *statistic variable*. Statistics variables are simple statistics that are added automatically. You can also create user-defined statistics to include in the summary.

The following example shows how to create a summary that provides an overview of the OWNER fields for each CLASS, and the QUAL fields for each CLASS, OWNER combination. This summary can be created using a three-level summary: CLASS by OWNER by QUAL. The CARLa statement to product this report is: SUMMARY CLASS * OWNER * QUAL.

Table 316 shows the results of the three-level summary using the example data.

Table 316. Three-level SUMMARY report - CLASS data summarized by OWNER and then QUAL value for eight records

Class	Owner	Qual	Count (Statistics variable)
DATASET			8
	ONE		3
		SYS1	1
		SYS2	2
	TWO		5
		SYS1	2
		SYS2	3

CARLa command statement: SUMMARY CLASS * OWNER * QUAL

Reviewing the results shown in Table 316, this summary report provides a count of all DATASET records (eight). This example shows that extra summary levels do not add any values, but add more statistic information. When user-defined statistics

are added such as minimum value, maximum value, counts, and average value, additional summary levels display additional statistics, thereby giving a better overview of the data.

The example in Table 316 on page 920 was created using a simple SUMMARY command. The following example shows how to mix raw data with the summary data, interleaving the KEY field data with the summary and statistics data. The CARLa code to produce this report is:

```
SORTLIST key
SUMMARY CLASS * OWNER * QUAL
```

Table 317 shows the results of this type of report using the example data.

Table 317. SUMMARY report that includes summary information mixed with raw data

Class	Owner	Qual	Count	Key (Detail lines)
DATASET			8	
	ONE		3	
		SYS1	1	
				SYS1.ONE.AA
		SYS2	2	
				SYS2.ONE.AA
				SYS2.ONE.BB
	TWO		5	
		SYS1	2	
				SYS1.TWO.AA
				SYS1.TWO.BB
		SYS2	3	
				SYS2.TWO.AA
				SYS2.TWO.BB
				SYS2.TWO.CC
SORTLIST key SUMMARY CLASS * OWNER * QUAL				

Table 317 shows that the non-summarized **KEY** data is included as *detail lines* , indented to the right of the summary. Detail lines do not have any summary statistics.

These examples show some of the basic features of the SUMMARY command. You can find information on other available features and additional examples by selecting a topic from the SUMMARY command introduction. (See “SUMMARY” on page 918.

Summaries in batch and ISPF

Use the SUMMARY command to create interactive summaries in ISPF and summary reports in either batch or ISPF. You can use this command within the context of a NEWLIST statement in combination with a DISPLAY command (interactive summary) or SORTLIST command (summary report) to include detail data.

Statistic or boolean variables to be included in a summary report are defined by the DEFINE command. (see “DEFINE” on page 750); the output modifiers that can be used in a summary are described with the LIST command (see “LIST family of commands” on page 794).

The SUMMARY command can be used for interactive and batch summary reports; it has an equivalent, DSUMMARY, which always generates interactive summaries. The behavior of the commands is detailed in the following table.

	SORTLIST	DISPLAY	No detail
DSUMMARY	ISPF	ISPF	ISPF
SUMMARY	file	ISPF	file

The DSUMMARY command always generates an interactive ISPF summary, while the SUMMARY command only does so when combined with DISPLAY.

Summary terms

The basic concept in a summary is the summary level. A summary level is a combination of one or more fields used as summary key; every key value is kept once per summary level, and is crossed with the summary levels above and below. In the preceding summary examples, first (CLASS OWNER) and QUAL were used as keys; later CLASS, OWNER, and QUAL were used. The (CLASS OWNER) combination is called a compound key.

In the SUMMARY command, summary levels are separated by an asterisk (*). Each summary level must contain at least one key variable. A field is always a valid key variable, unless it has been converted to a statistics variable by using one of the key modifiers listed in Table 318 on page 924. Other valid key variables are define variables of the types in Table 289 on page 754. DEFINE variables of the type listed in Table 288 on page 753 are statistics variables. Statistics variables can be included in the SUMMARY command, but they are not valid key variables.

In an ISPF display, each summary level has its own display panel; in a batch report, each summary level has its own output line. The examples at the end of this section show output from sample summary reports; for an example ISPF summary, see menu option **AU.S** Status audit.

The following example shows a simple SUMMARY command, summarizing CLASS by OWNER by QUAL. This example does not include user-defined statistic variables; as described in the following text, a '**Count**' statistic is added automatically to each level.

```
newlist type=racf
 summary class * owner * qual
```

The following example shows a summary command with one summary level and two statistics: a count and a relative frequency. The example lists all classes in the RACF database, the count of profiles encountered per class, and the relative frequency of each class:

```
newlist type=racf
 define cnt count
 define frq freq
 summary class cnt frq
```

Summary types

When the SUMMARY command is used within a NEWLIST and no SORTLIST or DISPLAY appears before the SUMMARY command, the summary does not include any detail information. If a SORTLIST or DISPLAY command precedes a SUMMARY command within the same NEWLIST, the summary is mixed with detail information from the SORTLIST or DISPLAY.

When SUMMARY and SORTLIST are combined, the resulting summary is a report containing summary lines followed by those SORTLIST lines described by the last summary line. Such a summary report can be generated both in batch mode and using ISPF.

When SUMMARY and DISPLAY are combined, or DSUMMARY and SORTLIST, the resulting summary is an ISPF summary, where the relevant detailed information from the DISPLAY command is included as the lowest summary level. This kind of report is only possible using ISPF.

When a SUMMARY command is used without a preceding DISPLAY or SORTLIST command, the resultant summary is a report. Use the DSUMMARY command for an ISPF summary.

The following example shows the use of the SUMMARY and SORTLIST commands combined. The resultant summary report selects all profiles of class DATASET matching the filter SYS%.** (e.g. SYS1.BRODCAST). The resultant summary report contains one summary line for each first-level qualifier and a count of the profiles selected, followed by a list of the profiles and the profile type.

```
newlist type=racf
 select mask=sys%.** class=dataset segment=base
 sortlist key proftype
 summary qual
```

Repeat groups

When repeat groups are summarized, each occurrence of the repeat group is summarized. If a value occurs several times within a single repeat group, every instance is counted. The output of these multiple occurrences can be suppressed by the NEWLIST NODUP parameter. The way repeat groups are summarized has several implications:

- When a summary is combined with detail information, the same detail profile or record is repeated in the output for each different repeat group value. E.g. if a repeat group has values ONE and TWO, the detailed information is included both with ONE and with TWO.
- Detail information is counted once for every summary key it is combined with. If repeat groups are summarized, lowest-level counts might not seem to add up, since a detail occurrence is counted multiple times on lower summary levels, but is counted once on the higher (non-repeat group) summary levels.
- When the NEWLIST NODUP parameter is used, the output does not contain duplicates. NODUP applies both to the input of the summary (duplicates are eliminated before the summary) as to the detail level (duplicate lines are removed, but they are counted, for instance when summarizing a repeat group field).

Statistic variables

Summary reports can contain statistics variables. These variables can be defined by a prior DEFINE command or by using one of the field modifiers, listed in

Table 318, on a field of the (D)SUMMARY statement. Each statistic variable can be limited to one or multiple summary levels. When a statistic variable applies to multiple levels, each level is independent: each summary variable describes the instances summarized by its own level. The following example has two summary levels. The highest summary level summarizes classes and the count of records per class. The second summary level summarizes first-level qualifiers and the number of records for each.

```
newlist type=racf
 define profcnt count
 summary class profcnt * qual profcnt
```

A statistic variable propagates to all higher summary levels, unless a NOPROP output modifier is used. If the lowest summary level does not contain a statistic variable, a count variable is added that propagates to all higher summary levels.

Table 318 lists the DEFINE statistics that can be specified as field modifiers for the DSUMMARY or SUMMARY commands.

Table 318. Statistics that can be specified for the (D)SUMMARY commands

Kind	Category	Meaning
AVG AVERAGE	field	Average of fields summarized.
FREQ FREQUENCY	occurrence	Percentage that the condition clause evaluates to true among occurrences (when combined with a condition clause), or percentage of occurrences selected (without a condition clause).
MAX MAXIMUM	field	Maximum of fields summarized.
MIN MINIMUM	field	Minimum of fields summarized.
CPRX COMMON_PREFIX	field	The common prefix of the fields summarized. If the fields are the same then the field value will be displayed. If a (remove hard breaks) common prefix was found, the common prefix is displayed followed by a ">", for example, SYS>. If a common prefix is not found, either "+" or "<more>" is displayed.

Suppressing lower summary levels

A summary level and all its lower summary levels can be suppressed by giving all summary keys of that level the NONDISPL attribute. This works on all summary levels except the top one. Sometimes you just want to summarize on a field and know how many different values there are, but not see those values. For instance, when analyzing your 3 RACF databases, you might want to know how many different user IDs there are. A query like

```
n type=racf
 def #userids sumcount
 s c=user s=base
 summary class #userids * profile
```

will show you the desired number, but also all individual user IDs summarized over all complexes. By adding the NONDISPL attribute (abbreviated ND), you can signal you want to suppress those lines:

```
n type=racf
 def #userids sumcount
 s c=user s=base
 summary class #userids * profile(nd)
```

This will give just one line of output.

Conditional clauses for statistic variables

Statistic variables defined with the DEFINE command might have a condition, a so-called WHERE clause. The WHERE clause is evaluated for each occurrence that is summarized; the variable is only updated if the WHERE clause is true. This allows you to describe data or conditions that are not included in the summary itself, but that can be gathered from the data summarized.

In the following example, a summary is created of all SYS%.** profiles by owner. The variable FRQ shows the percentage of profiles with a UACC of NONE. Note that FRQ is only included on the highest summary level; the count variable PRF is included on the lowest level, and is propagated to the highest level.

```
newlist type=racf
 select class=dataset mask=SYS%.** segment=base
 define prf count     /* Profile count */
 define frq freq where(uacc=none)
 summary qual frq * owner prf
```

For more information about WHERE clauses, refer to the DEFINE command "DEFINE" on page 750.

Thresholds

Thresholds can be used to select only those summary lines (and related detail information) that contain a statistic variable matching a numerical threshold. Thresholds might only be specified for numerical statistic variables. In the following example, only those summary and detail lines for qualifiers with more than 10 data set profiles are printed:

```
newlist type=racf
 define profcnt count
 select class=dataset segment=base
 sortlist key proftype
 summary qual profcnt(>10)
```

Note that a threshold does not change the value of the statistic variables, sums and counts; it merely hides those summary lines (and underlying summary levels or detail information) that do not match the threshold.

The following types of thresholds might be specified: >, <, >=, and <=. Per summary level, each statistic might have only one threshold; however, you might specify several summary variables with thresholds per summary level.

Warning. By default, a threshold propagates with the statistic variable to higher summary levels. This means the same numerical threshold is also applied to the higher summary levels. For the < and <= thresholds, this may lead to unexpected results, since statistic variables like COUNT and MAX tend to be larger at the higher levels. If you do not want to apply the threshold at higher summary levels, specify the NOPROP output modifier, or specify the same variable, with a different threshold, on the higher summary level.

Overriding length

When a key variable in a SUMMARY command is used with an overriding length, the effect is dependent on the output type. If the field is a string, the overriding length is used during summary processing; if the field is not a string, the overriding length is only used during output.

If the overriding length is used during summary processing, only the first part of the key variable is used, as specified by the overriding length. So, if user ID(4) is used in a summary, all user ID fields that have the first four letters in common are treated as a single summary case.

An overriding length of zero makes no difference during summary processing (the full key, trimmed of trailing blanks, is used), but makes a difference with printing summary reports (non-ISPF). Each summary key that has overriding length zero shifts the detail lines to the left, allowing more detail information to fit on the output line. Use this option with care because it can reduce report clarity.

Changing the sort order

A summary is sorted level by level, column by column, in ascending order. The sort order can be changed by using the output modifier DESCENDING; this causes a column to be sorted in descending order. This output modifier can also be used on the SORTLIST fields, if detail information is included. The following example shows a summary sorted on ascending class and descending owner:

```
summary class * owner(descending)
```

You can also sort on a statistic variable. However, the variable must be included *before* the key variables for this to work. If you want to sort on a statistic variable, but want to display it behind the key variable, use the NONDISPLAY output modifier. The following examples show a summary sorted on count, one with the count displayed before the key variable, and one with the count behind the key variable. The NOPROP output modifier makes sure that the count is displayed on the lowest summary level only.

```
newlist
 define #owner(noprop) count
 summary class * #owner owner

newlist
 define #owner(noprop) count
 summary class * #owner(nondisplay) owner #owner
```

Indirect references in a summary

When using indirect references (see “Indirect reference or lookup” on page 764) in a summary, the summary is performed on the base value of the field, while the referenced value is printed. For example:

```
summary userid:name
```

performs a summary on user ID. Even though several users have the text 'TESTUSER' in the name field, they will appear on different summary lines.

Deciding which complex is meant to be used for the indirect reference can be rather involved in a summary:

```
newlist type=trusted
sortlist auditpriority auditconcern
summary userid_complex userid userid:name * complex resource
```

The field *complex* is the security database (complex) associated with the resource, the field *userid_complex* is the security database (complex) to which the user ID belongs.

The *complex* fields have to be added to make it possible for the summary processing to intelligently decide which security database contains the data needed in each case.

Security zSecure decides which complex to use as follows: Any summary field that has a name ending in 'complex' is considered to contain a complex name and is used to decide which complex to perform the indirect reference. First the summary level containing the reference is checked to see if it contains a complex field. If so, it is used. If not, the higher summary levels are tested in sequence, until one such field is encountered. If there are multiple complex fields on a single summary level, the first at the same level is used.

If no complex fields are found in the current and higher summary levels, the default complex, as mentioned in message CKR0615, is used.

Rules and restrictions

The following rules and restrictions apply to the SUMMARY command:

- At least one key variable must be per summary level, that is not just statistic variables.
- When a summary level has more than one key (a *compound key*), none of the key variables can be repeated fields.
- It is not possible to summarize statistic variables.
- It is not possible to summarize on look-up variables. As a result, the command `SUMMARY USERID:PGMRNAME` summarizes on user ID.
- Do not summarize on a repeated field if that repeated field is also included in the detailed information. If you try this type of summary, the summary processing requires a vast amount of memory. Use the NEWLIST NODUP parameter to cut down on memory use.
- The SUMMARY command can not be used in a MERGELIST/ENDMERGE.
- The EXPLODE and RESOLVE output modifiers cannot be used.

Conversions

Conversions can be used to replace segment name qualifiers of SUMMARY key field values with fixed characters. See the “CONVERSION” on page 737 CARLa command.

The general syntax for conversion application is as follows:

```
field(CONVERSION(conv1[,conv2...]))
```

In the following conversion example, conv1 is applied to the SUMMARY key field RESOURCE, then conversion conv2 is applied to the result, and so on. The conversions conv1 and conv2 are defined by the CONVERSION command (abbreviated as CONV).

```
newlist type=ACCESS
summary resource(CONVERSION(conv1[,conv2...])) class
```

Using the summary statement - examples

For examples using the summary statement with different types of data, formats, and options, choose from the following topics:

Example - basic summary

The following example shows a basic summary. All discrete data set profiles are summarized by high-level qualifier and owner. No detail information or summary statistics are included; a count statistic is added by default. The count for qualifier C#MA indicates that 3 discrete profiles start with C#MA, of which 2 are owned by C#MAINT and 1 is owned by C#MASCH.

```
newlist type=racf
 select discrete class=dataset segment=base
 summary qual * owner
 QUAL     Owner    Count
 BZOPRDG                1
          BZOPRDG       1
 C#MA                   3
          C#MAINT       2
          C#MASCH       1
 C#MBERT                4
          C#MBERT       4
 RDIVALG                1
          RDIVALG       1
 RDPSDAB                2
          RDPSDAB       2
 RDPSKAE                1
          RDPSKAE       1
 SYSHSM                20
          BZOPRDG       1
          C#MAINT       2
          C#MASCH       3
          C#MBERT       3
          RDIVALG       1
          RDOPHEG       6
          RDOPTRY       1
          RDPSDAB       2
          RDPSKAE       1
```

Example - apply thresholds

In the following example, the same data is summarized, but only those summary lines are included that show the high-level qualifiers with more than one profile, and the owners with more than one profile in a HLQ.

```
newlist type=racf
 select discrete class=dataset segment=base
 define cnt count
 summary qual * owner cnt(>1)
QUAL     Owner    CNT
C#MA                    3
         C#MAINT        2
C#MASCH                 2
         C#MASCH        2
C#MBERT                 4
         C#MBERT        4
RDPSDAB                 2
         RDPSDAB        2
SYSHSM                 20
         C#MAINT        2
         C#MASCH        3
         C#MBERT        3
         RDOPHEG        6
         RDPSDAB        2
```

Example - sort on statistic variables

In the following example, the same data is summarized again, this time sorted on descending profile count, then on qualifier and owner.

```
newlist type=racf
 select discrete class=dataset segment=base
 define cnt count
 summary cnt(descending) qual * owner
CNT      QUAL     Owner    Count
      20 SYSHSM                20
                 BZOPRDG         1
                 C#MAINT         2
                 C#MASCH         3
                 C#MBERT         3
                 RDIVALG         1
                 RDOPHEG         6
                 RDOPTRY         1
                 RDPSDAB         2
                 RDPSKAE         1
       4 C#MBERT                 4
                 C#MBERT         4
       3 C#MA                    3
                 C#MAINT         2
                 C#MASCH         1
       2 RDPSDAB                 2
                 RDPSDAB         2
       1 RDIVALG                 1
                 RDIVALG         1
       1 RDPSKAE                 1
                 RDPSKAE         1
```

Example - summary with detail information

In the following example, the discrete data set profiles starting with C are summarized; this time, a SORTLIST is specified before the SUMMARY in order to include detail information with the profile key and UACC.

```
newlist type=racf
 select discrete class=dataset qual=c* segment=base
 sortlist key uacc
 summary qual * owner
```

```
QUAL     Owner    Count    Profile key                                UACC
C#MA                    3
         C#MAINT        2
                          C#MA.C#MPROD.LOAD                          NONE
                          C#MA.C#MTEST.LOAD                          NONE
         C#MASCH        1
                          C#MA.QUALOWN                               NONE
C#MBERT                 4
         C#MBERT        4
                          C#MBERT.GDGMODEL                           NONE
                          C#MBERT.SYS1.CAUMODEL                      NONE
                          C#MBERT.SYS1.CAUNVSAM                      NONE
                          C#MBERT.SYS1.CAUVSAM1                      NONE
```

Example - summary statistics

In the following example, all data set profiles matching the mask SYS%.** are summarized by UACC. The variable FRQNON shows the frequency (percentage) where the UACC is NONE. Note that the variable COUNT is added automatically, since no summary statistics were included at the lowest summary level.

```
newlist type=racf
 select mask=sys%.** class=dataset segment=base
 define frqnon freq where uacc=none
 summary qual frqnon * uacc
```

```
QUAL     FRQNON   UACC    Count
SYS1           31               44
                  NONE          14
                  READ          28
                  UPDATE         2
SYS2            5               17
                  NONE           1
                  READ          12
                  UPDATE         3
                  CONTROL        1
```

Example - overriding length

In the following example, the discrete data set profiles of the owner are summarized on the first four characters; then the full owners are summarized again.

```
newlist type=racf
 select class=dataset discrete segment=base
 summary owner(4) * owner
```

```
Owne Owner    Count
BZOP                2
     BZOPRDG        2
C#MA               10
     C#MAINT        4
     C#MASCH        6
C#MB                7
     C#MBERT        7
RDIV                2
     RDIVALG        2
RDOP               15
     RDOPHEG       10
     RDOPROB        2
     RDOPTRY        2
     RDOPTST        1
RDPS                6
     RDPSDAB        4
     RDPSKAE        2
```

Example - overriding length zero

In the following example, an overriding length of zero is used. The SUMMARY command summarizes on the full length of the data, but include the detail data as if the summary has length zero. This can be used to fit more data onto a line; since the output becomes rather less clear, you should use this option with care.

```
newlist type=racf
 select class=dataset discrete segment=base
 sortlist key
 summary qual(0) * owner(0)
```

```
  Count    Profile key
BZOPRDG         1
 BZOPRDG        1
           BZOPRDG.FORT.LOAD
C#MA          3
 C#MAINT        2
           C#MA.C#MPROD.LOAD
           C#MA.C#MTEST.LOAD
 C#MASCH        1
           C#MA.QUALOWN
C#MASCH         2
 C#MASCH        2
           C#MASCH.TESTGDG.G0002V00
           C#MASCH.TESTGDG.G0003V00
C#MBERT         4
 C#MBERT        4
           C#MBERT.GDGMODEL
           C#MBERT.SYS1.CAUMODEL
           C#MBERT.SYS1.CAUNVSAM
           C#MBERT.SYS1.CAUVSAM1
RDIVALG         1
 RDIVALG        1
           RDIVALG.DARTS.MACLIB
RDPSDAB         2
 RDPSDAB        2
           RDPSDAB.PR.TEXT
           RDPSDAB.STRT.CLIST
RDPSKAE         1
 RDPSKAE        1
           RDPSKAE.ISPPROF
```

Example - getting rid of an extraneous leading blank

When a NEWLIST specifies both a SORTLIST and a combination of SUMMARY with the newline character /, each line is preceded by a single blank. This can be overridden by adding a "|" between the SORTLIST and the first field. For example:

```
newlist
s c=user s=base
sortlist | key(8)
summary class count /
```

SUPPRESS

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

Use the SUPPRESS command to stop the following types of processing:

- Verification of failure messages
- Command generation
- Scoping rules that are used in REPORT SCOPE or NEWLIST SCOPE statements

The SUPPRESS command is global in scope and applies to all commands. You can abbreviate the SUPPRESS command as: SUP, SUPP, or SUPPR.

Suppressing verification messages is useful if your installation has full-volume copies of critical volumes on hot standby with a different volume label, or emergency copies of the master catalog.

If you supply at least one CKFREEZE file, the following commands act on some resources and the profiles that protect them: COPY, MOVE, REMOVE and VERIFY commands. If you do not want to permit these operations, you can use the following SUPPRESS command to prevent them from changing the RACF database: SUPPRESS DELETEDATASETS COPYALIAS When this command is run, all resource deletion, catalog alias and copy operations are suppressed. As a result, zSecure does not generate the corresponding commands to change the RACF profiles nor does it read the CKFREEZE file when any of the following commands are run: COPY, MOVE, REMOVE, or VERIFY.

You can also stop certain types of processing on specified volumes and catalogs by using the CATALOG and VOLUME keywords with the SUPPRESS command.

Using SUPPRESS VOLUME has the following effects on processing:

- The volume is not processed.
- Catalogs residing on the volume are not processed, which is useful to prevent processing on a hot standby volume.
- Resource deletion commands for the specified volume have no effect.

However, using SUPPRESS VOLUME can cause errors related to resource deletion. Because Security zSecure considers a VSAM cluster to be an atomic entity, it does not consider cluster components on other volumes as separate entities. If you delete a cluster that has components on an excluded volume, the cluster is not deleted. This can cause VSAM inconsistencies that show up as error messages that need to be resolved using the IDCAMS DIAGNOSE command. Similarly, an apparent orphan NVR is not removed.

Note: The IDCAMS DIAGNOSE command requires special privileges to run under SMS.

If you exclude a catalog, zSecure does not generate any commands for that catalog. This can imply that ALLOCATEand FREE commands are generated to delete non-VSAM DSCBs for data sets appearing uncataloged. You can suppress this behavior by specifying the DELETEUNCATALOGED parameter. Note that DEFINE and DELETE ALIAS commands are issued against inactive master catalogs as well as active ones, insofar as they are addressable from the current system and are not excluded.

If you suppress resource deletion, no other messages are issued about the suppression. In addition, attempts to delete resources are not counted as suppressed.

If you decide to suppress only deletion of uncataloged data sets or delete commands specifying the NOSCRATCH keyword, the SYSPRINT still includes messages for those operations showing the commands that are generated if the delete command was permitted. You can explicitly exclude these messages by issuing a SUPPRESS command to stop the CKR0720 and CKR0727 messages.

Note: The NOSCRATCH keyword requires special privileges to run under SMS.

Because resource management avoids the use of the CATALOG keyword on IDCAMS commands, do not attempt to run the CKRCMD with an active master catalog that is different than the one that was current during the command generation.

Note: The CATALOG keyword requires special privileges to run under SMS.

If you need to re-run a command from another system, update the CKFREEZE files before running the command. Note that the following data sets are deleted:

- Data sets residing under a removed profile
- Data sets with a high-level qualifier (HLQ) matching the ID
- Data sets with a HLQ not protected by a profile

Data sets with a HLQ not protected by a profile exist if all data sets were not removed before removing the RACF profiles.

SUPPRESS command options

The SUPPRESS command provides a number of options that can be used to stop processing of verification of failure messages, command generation and scoping rules for use in REPORT SCOPE or NEWLIST SCOPE. These options are described in this topic. Some of the options, such as VOLUME, CATALOG, DELETEUNCATALOGED, and DELETEDATASETS are discussed in the introduction to the SUPPRESS command (“SUPPRESS” on page 932).

ACCESS_GDG_VERSION
To reduce the size of consolidated Access Monitor data sets, this option maps the G*nnnn*V*nn* qualifier of GDG generation resource names into a fixed string of GnnnnVnn for all TYPE=ACCESS input records. For example, G1259V00 is mapped to GnnnnVnn.

ACCESS_JESSPOOL_JOBID
This option is checked when reading TYPE=ACCESS input files. This SUPPRESS option converts the fourth JESSPOOL resource name qualifier (the job ID) into a

fixed string by using the following convention: the leading S, J, or T character is retained and the remaining characters in the job ID are replaced with a lowercase x.

ACCESS_JESSPOOL_DSID
This option is checked when reading TYPE=ACCESS input files. This SUPPRESS option converts the fifth JESSPOOL resource name qualifier (the data set ID) into a fixed string if it starts with a D by using the following convention: the leading D character is retained and the remaining characters in the data set ID are replaced with a lowercase x; if the data set ID includes a word such as GROUP, the word GROUP is retained as part of the resource name qualifier.

ADDSD
ADDDSD
ADD
Limits the commands generated by the COPY command to exclude the addition of data set and general resource profiles as well as profile members. For example, on a COPY USER=*user ID* TOUSER=*id* command, you can use this option to prevent the addition of data set profiles starting with *id* to the copy command.

AUTO_RESOURCE
The AUTO_RESOURCE parameter specifies that resource simulation operations are limited to the resources that are explicitly specified by SIMULATE commands. Resources that are determined from CKFREEZE data sets are not automatically included in the analysis.

CATALOG= *catname*
CAT=*catname*
This option suppresses error messages related to this catalog. In addition, resource copying and deletion will not take the contents of this catalog into account, so no IDCAMS commands will be (implicitly or explicitly) directed to it; this might lead to some data sets appearing uncataloged and being scratched from the VTOC directly (see DELETEUNCATALOGED).

CONNECTOWNER
Do not use the RACF connect owner field of group, user, or connect profiles during VERIFY PERMIT, REMOVE PERMIT and MERGE processing. For VERIFY PERMIT and REMOVE PERMIT this has the effect of not generating CONNECT commands to change the connect owner when it is a user ID or group which no longer exists. For MERGE operations no commands will be generated to set the connect owner field to any specific value.

COPYALIAS
Suppresses the generation of IDCAMS DEFINE ALIAS commands by COPY. This option is implied by SUPPRESS CKFREEZE. It is also automatically implied if no CKFREEZE file is allocated.

COPYCUSTOMDATA
COPYCSDATA
Suppress the generation of RACF commands to copy custom fields.

COPYUSERDATA
COPYUSRDATA
Suppress the generation of CKGRACF commands to copy user data.

DBIDCACHE
Suppress the translation of DB2 DBID, OBID, PSID, and DSID numbers to their respective database names, table space names, table names, and data set names. Some SMF type 100/101/102 record subtypes contain definitions of specific ID

numbers (namely, 24, 104, 105, 107, 142, 143, 144, and 258) and the bulk of the subtypes only refers to the objects by their numeric ID number. By specifying this option you can see what the SMF records really contain. The main use of this option is to assist in diagnosing problems in DB2_OBJECT and RECORDDESC that can be caused by providing the wrong order of SMF records or SMF with gaps. DB2 immediately reuses object ID numbers for new objects after an object has been deleted, and IBM Security zSecure cannot cope unless the SMF records are read in the proper order.

CKFREEZE
CKFREEZE IOCONFIG
Suppress the use of a CKFREEZE file with catalog information. This is useful for commands that would need CKFREEZE data to guarantee completeness and correctness of information about VSAM profiles, but also provide a lot of useful information without this info. If a cursory analysis is sufficient, you can save a lot of time by omitting the CKFREEZE file for analysis. For zSecure Audit for ACF2, this parameter is ignored for NEWLIST TYPE=SMF in restricted mode, and message CKR0521 is issued.

DELDSD
Limit the commands generated by REMOVE and MOVE operations to exclude deletion of data set profiles as well as other profiles or profile members to be removed. For example, on a REMOVE USER=*user ID* command, the deletion of all profiles starting with *user ID* can be prevented by specifiying this option. Note that this probably results in failure of a DELUSER command. If this parameter is specified, generation of DELGROUP commands that fail due to still existing data set profiles is suppressed. Message CKR1062 is issued to warn you that the command generation was suppressed.

DELETEDATASETS
To suppress the generation of all non-RACF commands by MOVE, REMOVE and VERIFY to delete data sets and catalog aliases. As a result, it might become unnecessary to read the CKFREEZE, which can gain you speed. This option is implied by SUPPRESS CKFREEZE; in turn it implies SUPPRESS DELETENOSCRATCH and DELETEUNCATALOGED. This option is also automatically implied by the absence of the CKFREEZE file.

DELETENOSCRATCH
Suppress the generation of IDCAMS DELETE commands with the NOSCRATCH keyword. A suppression message is issued instead of generating the commands. The NOSCRATCH keyword is only generated if a DELETE without it is not possible, because the data set is in several catalogs for example. Migrated data sets do not require this keyword. This option is implied by SUPPRESS DELETEDATASETS.

DELETEUNCATALOGED
To suppress the generation of ALLOCATE and FREE commands to scratch uncataloged data sets from the VTOC; if you want to supply the resource deletion commands to IDCAMS directly (instead of via TSO), you should specify this option, since IDCAMS only partially supports ALLOCATE and does not support FREE at all. This option is implied by SUPPRESS DELETEDATASETS.

ECKD
This parameter request fallback to non-ECKD channel program formats to be used with EXCP access to the RACF data sets. This reduces the size of sequential I/O operations from 3 tracks to 1 track.

FALLBACK
Suppress flagging second order error conditions. Presently this only affects VERIFY STC, where it means that ICHRIN03 entries are only verified for referential integrity when used (unused entries will still be flagged as such); note that currently unused STARTED profiles are never syntactically verified.

FMTABEND
Suppress user abend 931 which follows error message CKR0931, indicating a buffer overwrite in a text formatting procedure.

ICHCNX00
Suppress invocation of this RACF exit to determine the first qualifier. This command might be necessary if the exit depends on key 0 operation. This option is activated automatically if an abend condition is intercepted while calling the exit.

This option might also be required for processing data from another system. In this case, the `ICHCNX00` of the current system is used, not that of the subject system. This processing works if the systems have the same level of `ICHCNX00` exit code. If the systems do not have the same level exit, it might be better to suppress `ICHCNX00` processing.

The SUPPRESS ICHCNX00 command is not supported in restricted mode.

ICHNCV00
Suppress the use of the RACF naming convention table `ICHNCV00` in RACF and SMF reporting. The table normally used is the copy in the CKFREEZE file.

ICHRRNG
Suppress use of the RACF range table. This table maps the profile key to a specific RACF data set sequence number. The table used is the copy in the `CKFREEZE` file, unless the data source is a live RACF database. For a live database, the live `ICHRRNG` is used. Typically, profiles in the 'wrong' RACF data set are not seen by RACF and the IBM Security zSecure products. When you specify SUPPRESS ICHRRNG the profiles are processed and can be identified. This setting can cause messages to be issued for duplicate profiles, class not in CDT, and connect inconsistency, and other messages. Also, the pseudo field INRANGE can be used to identify the profiles.

ID= *id*
Suppress error messages and report lines concerning this user or group. In the case of multi-line messages, sometimes only the line containing the message id is suppressed.

INDEX
This parameter suppresses use of the RACF data set index and causes a sequential read.

INDEXCUTOFF
This option is for debugging and performance analysis purposes. It suppresses automatic fallback to sequential `I/O` in a RACF data set if the program gauges the number of indexed I/O requests to take longer. Because specifying this option can increase the elapsed time for some queries by more than a factor 12, do not use it with very large databases. Experience shows that queries that select 100,000 or more profiles perform badly while in indexed I/O mode. See also “LIMIT INDEXBIAS” on page 789.

The specification has no effect when `BDAMQSAM` has been specified. This option implies `SUPPRESS DELETEDATASETS` and `COPYALIAS`

MANAGERACFVARS
To suppress interpreting keys and members in RACFVARS profiles to represent users and groups wherever they match a defined user or group id, and have COPY, MOVE and REMOVE generate commands accordingly.

MSG= *list*
MESSAGE=*list*
A single decimal message number or a list of decimal message numbers enclosed in parentheses and separated by commas can suppress messages CKR*nnnn* where *nnnn* is the decimal message number. Besides suppressing the message output, this also suppresses processing of the return code associated with the message. Hence, the use of this option to suppress a critical error message that would terminate the program, might result in processing to be continued inadvertently, which can lead to abend conditions. The main use of this option is to suppress messages inherent to your configuration that you know about, but do not want to clutter your output with on each run. A large number of messages that would allow circumvention of restricted mode processing cannot be suppressed.

MSGTIMER
This parameter can be used to force display of all status messages in sequence, even though this causes response time to increase. This is mainly useful for automated testing programs.

MYACCESS< *level*
Limits REPORT and NEWLIST output to profiles that you might access at least the level indicated. The levels that can be used are listed with the ACCESS parameter of the REPORT command, see "REPORT" on page 875. As an example, SUPPRESS MYACCESS<ADMIN restricts REPORT and NEWLIST output to those profiles you may administer, for example profiles that are owner of, or discretes that you have ALTER access over. This keyword does not take system-wide privileges like system special into account, since otherwise it would make no difference whether the keyword was specified.

NOT_MY_LIST_SCOPE
This can be used to limit the profiles selected to those that fall within any scope specification including CKGLIST and AUDIT. The difference with SUPPRESS MYACCESS<ADMIN lies in the addition of profiles that can be reviewed due to CKGLIST scope or group-AUDIT authority.

RACF
Suppress the reading of the RACF database. This can only be used in unrestricted mode, and is useful if a NEWLIST is used that can make use of the RACF database, but does not require it. Typically, this is used in zSecure Audit for RACF.

REASON= *list*
Change REPORT SCOPE=, REPORT PERMIT=, or NEWLIST SCOPE=, reports to exclude profiles that would be included only for the reasons indicated. In restricted mode, the suppress reasons SELFCONNECT, PWDCHANGE, WARN, `NOPROFILE`, and `CKGRACMAP` are always set. Additional suppress reasons can be added as desired. See "Scoping rules that can be suppressed with REASON=" on page 938.

SETROPTSREFRESH
To suppress the generation of SETROPTS REFRESH commands.

SMF
Suppress the allocation of all SMF data sets. This can be used to prevent

unintended enqueues on and reads of the live SMF data sets while syntax checking a CARLa query. This is typically used when verifying an alert in IBM Security zSecure Alert.

SOFTEOF
Suppress soft end-of-file processing for ALLOC GETPROC routines. The soft end-of-file return code will be handled as a regular end of file.

UNIXCACHE
Suppresses the cache mechanism for the file path in calculating the effective file attributes (ATTR) for UNIX files.

VOL= *volser*
VOLSER=*volser*
VOLUME=*volser*
Suppress error messages relating to the specified volume. The volume is also ignored during resource copying and deletion. As a result, catalogs stored on the volume are also ignored which might make some cataloged data sets appear to be uncataloged and, as a result, scratched from the VTOC directly. (See 935.) If a Generation Data Group (GDG) is cataloged on this volume, neither the GDG or its Generation data sets (GDSs) residing on this volume are deleted. However, associated GDSs residing on other volumes might be considered uncataloged non-VSAM data sets and consequently scratched. VSAM components are never deleted separately. If you exclude one component, using the SUPPRESS option for example, you exclude the entire cluster.

Scoping rules that can be suppressed with REASON=

You can specify the following *list* values in the `SUPPRESS REASON=` *`list`* to suppress scoping rules:

ALTER-M
Suppress accesses that would be granted because users are permitted to modify certain fields of their own user profile ('alter myself').

CKGOWNR
CKGOWNER
CNGOWNR
CNGOWNER
Suppress accesses that would be included because access is granted through the CKGRACF authorized component of IBM Security zSecure Admin.

CKGRACMAP
Suppress access that is included because access through the CKGRACF authorized component of zSecure Admin is granted to FACILITY IRR.IDIDMAP.** resources.

CREATE
Suppress administrative access granted through CREATE authority on a connect and class authorization (CLAUTH) on a user.

GLOBAL
Suppress accesses that would be included because access is granted through the Global Access Table.

GRPAUDIT
GRPAUD
Suppress accesses that would be included because the user has the group-AUDITOR attribute.

GRPOPERATIONS
GRPOPER
Suppress accesses that would be included because the user has the group-OPERATIONS attribute.

GRPSPECIAL
GRPSPEC
Suppress accesses that would be included because the user has the group-SPECIAL attribute.

ID(*)
Suppress accesses that would be included because the access list grants access to the ID *, for example every RACF defined user.

NOPROFILE
UNPROTECTED
NOPROF
UNPROT
Suppress accesses that would be included because the data set or resource is not protected by a profile (in a NOPROTECTALL environment).

OWNER
Suppress accesses that would be included because (a) the user is owner of the profile; or (b) the first qualifier of a data set profile is equal to the user ID.

PWDCHANGE
PWD
Suppress accesses that would be included because another user ID, that is within the scope of the user, for example for which the password or password phrase can be set, is granted access on the access list, or is a direct owner.

SELFCONNECT
SELFCON
Suppress accesses that would be included because a group, that is within the scope of the user, for example to which the user can connect himself, is granted access on the access list.

UACC
UNIVACS
Suppress accesses that would be included because access is granted through the UACC.

WARNING
WARN
Suppress accesses that would be included because of profiles in warning mode.

Using the SUPPRESS command

The following examples show how to use the suppress command for different purposes. For an overview of the command, see "SUPPRESS" on page 932. For detailed information about the command options, see "SUPPRESS command options" on page 933.

Suppressing by volume: The following example shows how to suppress error messages for a dummy volume used for archived disk data sets.

```
suppress volume=migrat
```

Suppressing messages: The following example shows how to suppress error messages. This example suppresses the messages CKR072I and CKR073I.

```
suppress msg=(72,73)
```

Reducing scope output: The following example shows how to suppress common profiles in scope reports.

```
suppress reason=(global,uacc,id(*),warning,noprofile)
```

SYMBOLIC

The following information provides additions and corrections to the documentation for the LANGUAGE command which supports globalization of the zSecure product interfaces. This command is supported in the following zSecure products: Admin, Alert, Audit, Visual and the Tivoli Compliance Insight Manager Enabler for z/OS.

Use the SYMBOLIC command to define a symbolic name that can be used instead of a number. For example, you can use this command to define a symbolic name for a field length, a threshold specification, or a comparison against a numeric value in a SELECT statement. The symbolic name defined can be used directly as input during CARLa language processing (the CARLa input parse).

The following code sample shows the SYMBOLIC command syntax:

```
SYMBOLIC type  name=value
```

where

type
Specifies the type of symbolic. The only available type is NUM for numeric.

name=*value*
This parameter assigns a numeric value to the specified name which defines the *symbolic name*. The following syntax rules apply to the name=*value* specification.

- The name value cannot start with a digit (0 - 9, inclusive) and must contain at most 24 alphanumeric, national characters, or underscores.
- The *value* must be a base-10 (decimal) number. You cannot specify a hexadecimal (base-16) number.

During CARLa language processing, the symbolic name uses the assigned value until a SYMBOLIC statement with a matching name and type occurs in the input data. In the following example, the SYMBOLIC statement defines minvio=5. When the CARLa input parser encounters the summary statement, it interprets the *minvio* parameter as count (>5).

```
symbolic num minvio=5
...
summary ..  count(>minvio)
```

Multiple SYMBOLIC statements for the same name delineate the values used in the input parser. From the first definition of a symbolic name until the next definition for the same name, the assigned value is the one defined by the first SYMBOLIC statement. When a second SYMBOLIC statement with the same name is read, the value changes to the value specified in the second statement, and so on. For more information, see *Usage considerations*.)

The symbolic name can be used on its own or associated with a numeric default value as shown in the following example.

```
symbolic num minprio=40
...
select auditpriority>minprio|5
```

The default value is specified as `name|value` where *value* is a decimal number immediately following the vertical bar (|), without any spaces.

The vertical bar defines an OR relationship: Use the value from the SYMBOLIC statement if it is present, **or** use the default value from `name|value` if the SYMBOLIC statement is missing.

Usage notes

- You must define the symbolic name before the CARLa statement that references it. Otherwise, the definition is ignored.
- If the CARLa input processor expects a number or a symbolic name of type NUM for a `name`, and it encounters a non-numeric string that does not have a symbolic value defined, the following message is issued:
  `CKR1424: No numeric symbolic <name> found and no default at <ddname> line <line>.`
-

UNLOAD

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

The UNLOAD statement can be used to write selected profiles or records. This statement can be used with the following types of data:

- RACF
- ACCESS
- SMF

The unload of SMF and ACCESS data requires that the UNLOAD statement is inside the scope of a NEWLIST statement.

If the ddname CKRUNLOU is allocated, the unload of RACF or ACF2 data is an automatic default action in Security zSecure. You can use the ALLOC statement or allocation of files CKRACF01 through CKRACF*nn* to specify the source of the security database records. When used outside the scope of a NEWLIST, the UNLOAD statement does not support any parameters or keywords.

Use of a NEWLIST statement and an explicit UNLOAD statement is preferred. Using an explicit UNLOAD statement has the following benefits.

- In an MVS system, an error message CKR0002 is issued if no CKRUNLOU file was found.
- In a CMS system, the file named "FILE CKRUNLOU A" is created automatically if no GLOBAL CKRUNLOU was defined.

An UNLOAD statement can also be specified in the scope of a NEWLIST. In this case, records of the applicable NEWLIST TYPE are unloaded and the ddname parameter is required on the UNLOAD statement.

When using UNLOAD, the following rules applies:

- An UNLOAD statement within the scope of a RACF or ACF2_* NEWLIST cannot be combined with the SCOPE= parameter on the NEWLIST statement.

- In restricted mode, SMF records must be within the scope of your authority. For CICS SMF 110 monitor records, this implies that the CICS region userid must be within your scope.
- When an UNLOAD statement is used within an ACCESS NEWLIST, the Access Monitor data is processed in parallel and is also consolidated.
- Unloading Access Monitor data is only supported for Access Monitor records in V1.13 format. Access Monitor records in V1.11 format cannot be processed using UNLOAD.

The UNLOAD command has the following parameters:

DDNAME=*ddname*
DD=*ddname*
FILE=*ddname*
F=*ddname*
Output file name for records selected by this NEWLIST.

COMPLEX= *name*
Unload records from this complex. If omitted, the complex of the default system is used. This parameter is supported only for RACF and ACF2_* NEWLIST types.

VERIFY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

The VERIFY command can be used to check the consistency of the database internally as well as in relation to resource data collected by zSecure Collect. Commands to remedy the shortcomings found are generated if the CKRCMD file has been allocated.

There is one option to invoke all VERIFY options at the same time. This might cause excessive memory and CPU usage on very large systems.

ALL
Select all analysis parameters that are entitled at the same time.

In addition, the sort order of the error messages and generated commands might be changed. This is often a good way to detect related events.

BY= *list*
Keywords indicating error message sort order. Change the sort order only for reporting purposes: it is not guaranteed that the commands generated will be in the proper order unless the default sort order is used. The messages are always first sorted by complex, before any of the BY parameters take effect. The complex name is not always printed with the messages. *list* is a list enclosed in parentheses with the keywords separated by commas indicating one or more of the following sort fields (the order given is the default sort order):

MSG
Message type. This is an internal value (not the message number) that will cause messages to be sorted by issuing function (like VERIFY PROGRAM or REMOVE PERMIT) . In addition, similar messages will appear in groups. If MSG is first in the sort order (default), the messages for each issuing function start on a new page with a header indicating the function. Some

commands call more than one function, causing the output to be split across the functions called (like VERIFY ALL or REMOVE USER).

VOL VOLUME VOLSER
Volume serial.

DSN DATASET
Data set name (resource name).

PGM PROGRAM PROG
Program name (with AC1, PADS,PROGRAM, PGMEXIST, and STC).

ID PERMIT
User or group (permit). In VERIFY STC: the started procedure name.

Security database without CKFREEZE

VERIFY CONNECT, CON

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that the user, group, and connect profiles all provide the same connect information. No commands are generated to remedy the situation.

VERIFY GROUPTREE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that there are no loops in the group ownership structure in the database, e.g. group A owns group B owns group C owns group A... No commands are generated to remedy the situation, but the complete ownership loop is printed. A loop where user A owns group owns user A is *not* detected.

VERIFY PADS

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify the protection of programs in a conditional access list. Since z/OS 1.4, RACF can run in 3 program control modes: Basic, Enhanced-Warning and Enhanced. Basic program security is the default , and equal to pre-z/OS 1.4 RACF program security. Enhanced mode offers better security, but requires more work in setting up the PROGRAM profiles. See the RACF Security Administrator's Guide for more information about these modes.

For each mode, VERIFY PADS verifies different settings. In Basic mode it verifies if all programs used on conditional access lists have a matching PROGRAM profile. Running VERIFY PADS while running RACF in Enhanced-Warning mode or Enhanced mode verifies if all programs used on conditional access lists have a specific PROGRAM profile, and if such a profile has APPLDATA with 'MAIN' or 'BASIC'.

If a CKRCMD file is allocated, commands are generated to fix any problems found by the verify. Again, for the different modes, the generated commands are different. Beside fixing any problems in the settings, the generated commands can

help with converting from Basic program security to Enhanced program security. Below is an explanation on how to do this.

Before converting to Enhanced program security, first run VERIFY PADS while in Basic security mode. Commands are generated to delete conditional access list entries without a corresponding program profile. After review, run these commands. This should do no harm to your system because these entries would not give access anyway.

Put your system in Enhanced-Warning mode, or put SIMULATE RDEF FACILITY IRR.PGMSECURITY APPLDATA('ENHWARN') in the job or preamble (SE.3), and run VERIFY PADS again. The commands that potentially do damage to your system's settings are generated as comments. You have to decide which of the commands need to be uncommented. Read the RACF Security Administrator's Guide for more information.

- If a specific program profile is found for the WHEN-program but this profile does not have APPLDATA with 'MAIN' or 'BASIC', the program will generate a commented command to add APPLDATA('MAIN') on the specified program profile. You can uncomment the line if the program is a MAIN program. If the program should be a BASIC program, uncomment and change MAIN to BASIC. If the program is not needed anymore on the conditional access list, keep the command commented. This will result in having the conditional access list entry deleted when running VERIFY PADS in Enhanced mode.
- If no specific program profile is defined, but a non-specific match is found, the program will generate commands to copy the non-specific profile to a specific one, including the member list. Furthermore, the program adds APPLDATA('MAIN') to the profile. This series of commands (starting with an RDEFINE followed by indented RALTERs) must be uncommented if the program needs to be a MAIN or BASIC program. Change the second RALTER accordingly. Keeping the lines commented results in deletion of the conditional access list entry when running VERIFY PADS in Enhanced mode.
- If no non-specific profile is found for the WHEN-program, the program will generate commands to delete the conditional access list entry. If the VERIFY PADS run in Basic program security returned no messages, this situation will not occur.

After selecting which programs need to run in MAIN or BASIC security and uncommenting the appropriate generated commands, let RACF run in Enhanced-Warning mode for a while. Doing this will point out any problems that still exist with the configuration (like the need for additional programs on conditional access lists and program profiles with APPLDATA('MAIN') or APPLDATA('BASIC')).

When you are happy with the new configuration and RACF in Enhanced-Warning mode has been running warning-free for a while, put RACF in Enhanced program security mode. Run VERIFY PADS once more to delete all conditional access list entries that do not have a specific program profile with APPLDATA('MAIN') or APPLDATA('BASIC').

For more information about the messages you get while running VERIFY PADS and its associated commands, see the *IBM Security zSecure: Messages Guide*.

VERIFY PASSWORD

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•		

The VERIFY PASSWORD command checks the RACF database for hashed passwords and weak (easy to guess) DES-encrypted passwords. The results of a disassembly of the ICHDEX01 password encryption exit are taken into account (e.g. no DES-encryption is performed if all systems use hashing).

The VERIFY PASSWORD command does not work using an unloaded RACF database, since an unload does not contain encrypted passwords (or similar sensitive fields). Instead, a 'real' RACF database (a primary/back-up database, or a copy) is required. If the VERIFY PASSWORD command is used with an unloaded database, message CKR0590 is generated.

The VERIFY PASSWORD command does not compromise the weak passwords found; it lists the users that have a weak password, but does not list the passwords themselves. It generates messages CKR0584 through CKR0589.

The VERIFY PASSWORD command does not generate commands to correct any weak passwords found, because this is very much dependent on the security policy of the system. Some suggested actions are:

- Contact the user and ask him to change the password.
- Revoke the user.
- Change the password of the user.
- Expire the password of the user, so that the password must be changed a the next logon.
- Change the password policy of the installation: introduce a new-password exit, establish password rules, or set a strict password interval.
- Start auditing the user to check for suspect activity.

Instead of generating commands, the VERIFY PASSWORD command generates a query in the CKR2PASS file that can be used to select the user IDs with weak passwords. This query can be edited to report on the user IDs, or to generate commands as desired. You must then run Security zSecure again, using the edited query as input.

Note: We advise you to send the user *no email* notifying him of a weak password, or to notify the user in any other way using a computer system. If the email were to be read by hackers or eavesdroppers, this would seriously compromise the security of the system. Contact the user by telephone or using regular mail.

Security database with or without CKFREEZE

Use the `VERIFY PERMIT` action to report on the security database with or without a `CKFREEZE` file.

If the RACF database is part of a multi-system RRSF configuration and a CKFREEZE file is supplied along with the RACF databases for the other RRSF connected systems, then the VERIFY PERMIT command attempts to verify that a userid that is undefined on the current system is undefined on all the RRSF connected systems. If the userid is found to be defined on at least one other system in the RRSF configuration, then no commands are generated to cleanup the

references to the userid on the current system unless the ONLYAT option is specified. See "ONLYAT" on page 863 in the OPTION command documentation.

VERIFY PERMIT, PERM

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that each of the following is defined as a user or a group:

- ID entry in a standard or conditional access list
- owner
- RESOWNER
- NODES member
- superior group
- notify field
- STUSER and STGROUP specification other than =MEMBER in a profile with a generic first qualifier and certain APPLDATA fields

Also verify that users in keys of specially defined profiles (JESJOBS CANCEL.node.*userid*.jobname, for example) and data set profiles exist. This check pertains to the following classes:

- DATASET
- DLFCLASS
- CICS: TCICSTRN, GCICSTRN, DCICSDCT, ECICSDCT, FCICSFCT, HCICSFCT, ACICSPCT, BCICSPCT, JCICJCT, KCICSJCT, MCICSPPT, NCICSPPT, PCICSPSB, QCICSPSB, SCICSTST, UCICSTST, CCICSCMD, VCICSCMD
- FACILITY
- INFOMAN
- JES: JESJOBS, JESSPOOL
- LFSCLASS
- NODES
- PROPCNTL
- PTKTDATA
- STARTED
- SURROGAT
- TMEADMIN
- VM: VMCMD, VMRDR, VMBATCH, VMCONECT, VMEVENT, VMXEVENT

If the CKRCMD file has been allocated, commands are generated for the following:

- Delete permits, NODES members and profiles, STARTED user, groups and profiles that refer to non-existing ids.
- Change those OWNER, RESOWNER, NOTIFY, SUPGROUP and verified APPLDATA fields that refer to non-existing ids.

If a CKFREEZE is supplied, resource deletion is implied as well. That is, the data sets covered by the profiles are removed as well. (See "REMOVE" on page 870 and "SUPPRESS" on page 932 for details). The VERIFY PERMIT command is mutually exclusive with the COPY, MOVE, or REMOVE commands.

No commands and CKR0026 messages will be generated to change non-existing connect owners if SUPPRESS CONNECTOWNER has been specified. The reference count for undefined ids in message CKR0068 is **not** altered; undefined connect owners are still counted here.

Security database with CKFREEZE

VERIFY ALLNOTEMPTY, ALLNONEMPTY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

For a z/OS system, verify that all generic data set profiles cover real data sets. In addition to the NOTEMPTY option, profiles for which *no* less specific profile exists might also be flagged. If the CKRCMD file has been allocated, commands are generated to delete the empty profiles. If you have ABR configured to keep profiles, you are well advised to check if such an "empty" generic profile would cover a migrated non-VSAM data set if the assumption that it is RACF indicated on the migration tape turns out to be false. A CKFREEZE file is required.

This command supports RRSF configurations as follows:

- If the zSecure ONLYAT option **is not** specified, CARLa suppresses the generation of RACF commands that, if redirected, would cause deletion of a data set profile that covers existing data sets.
- If the zSecure ONLYAT option **is** specified, CARLa generates the DELDSD command that otherwise would have been suppressed and adds the ONLYAT parameter to generated RACF commands that should not be redirected; for example, commands that, if redirected, would cause deletion of a data set profile that covers existing data sets.

VERIFY DATASET, ONVOLUME, ONVOL

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

For a z/OS system, verify that each discrete profile has a corresponding RACF indicated data set. If ABR is configured to keep profiles, a non-VSAM data set migrated by it is assumed to be indicated. If the CKRCMD file has been allocated, commands are generated to delete the misleading (because unused) discrete profiles. A CKFREEZE file is required.

VERIFY INDICATED,IND

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that data sets with the RACF indicated bit on in the VTOC (non-VSAM) or catalog (VSAM) have a corresponding discrete DATASET profile, even if they seem to be covered by a generic profile. If the CKRCMD file has been allocated, commands are generated to first add discrete profiles with an access list that is a copy of the generic profile found (through use of the FROM parameter), and then delete the discrete profiles just created. This effectively removes the indicated bit. A CKFREEZE file is required.

Warning

The commands might be difficult to execute because commands involving the RACF indicated bit require en exclusive enqueue on the data set name. This is impossible to achieve for system data sets that are permanently enqueued.

For data sets migrated by ABR this verification is not performed in the current version of the product; if a non-VSAM data set had the RACF indicated bit set on migration, ABR will request a default discrete profile to be created via ADSP when the data set must be recreated on restore; migration of a VSAM data set does not preserve the RACF indicated bit.

VERIFY NOTEMPTY, NONEMPTY, GENERIC, GEN

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

For a z/OS system, verifies that generic profiles of the DATASET class are not empty, meaning that profiles protect existing data sets.

For a z/OS system, verify that generic DATASET profiles that are also covered by a less specific generic profile are non-empty, for example data sets exist that are covered by the generic profile. This is meant to remove obsolete generic profiles. You should be aware that profiles intended to prevent or allow *allocation* in a PROTECTALL environment (in a way that differs from the less specific profile) is also flagged as empty, while it might not be your intention to remove these profiles. [8] You might want to include SIMULATE SETROPTS TAPEDSN in preparation of setting this option, if it is currently not active or if the tape management system issues DASD-type checks. If the CKRCMD file has been allocated, commands are generated to delete the empty profiles. A CKFREEZE file is required.

This command supports RRSF configurations as follows:

- If the zSecure `ONLYAT` option **is not** specified, CARLa suppresses the generation of RACF commands that, if redirected, would cause deletion of a data set profile that covers existing data sets.
- If the zSecure `ONLYAT` option **is** specified, CARLa generates the DELDSD command that otherwise would have been suppressed and adds the `ONLYAT` parameter to generated RACF commands that should not be redirected; for example, commands that, if redirected, would cause deletion of a data set profile that covers existing data sets.

Warning:

Do not execute commands generated with an incomplete `CKFREEZE`. That is, a `CKFREEZE` made by a non-APF run of zSecure Collect. This will miss relevant VSAM information and will cause removal of profiles that cover (only) VSAM data sets. You are alerted to such dangers by the messages in the VSAM OR VVDS INCONSISTENCIES section of the output. Data

8. | For instance because the data sets have been archived, or because you have ADSP active, or because they are used for tape data sets, and the CKFREEZE file did not contain the relevant information.

sets mentioned in this section are usually not assigned to any profile because relevant information to do so reliably was missing.

VERIFY PGMEXIST, PROGRAMNONEMPTY, PROGRAMNOTEMPTY, PGMNONEMPTY, PGMNOTEMPTY

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that each PROGRAM profile covers at least one load module. To be covered by a profile, the name of the load module must match the pattern set by the profile key, and the load module must reside in a data set that is a member of the profile. If the CKRCMD file has been allocated, commands are generated to remove PROGRAM profiles that are not matched by any member or alias in any of the data sets in its member list.

If important information to decide whether there is a match is missing, the removal command is generated, but commented out. Messages in the SYSPRINT indicate why a certain decision was made. The messages are explained in detail in the *IBM Security zSecure: Messages Guide*.

To make sure the CKFREEZE file provides the appropriate information, follow these guidelines:

1. Include VTOCs for important volumes in a CKFREEZE data set so that zSecure knows what data sets reside on them. If you use DASD sharing, make sure that the set of CKFREEZEs for this complex contain the VTOCs of all DASD.

   For performance reasons, it is common to avoid duplicate VTOC information (in multiple CKFREEZE data sets) by running zSecure Collect with `SHARED=NO` on all except one of the z/OS images that share a set of DASD volumes. However, when a volume is shared among some, but not all of your z/OS images, and you run the CKFREEZE with `SHARED=YES` on an image that does not have access to that volume, that volume will be missing in the combined CKFREEZEs. The program's analysis is most reliable when analyzing all systems that share the RACF database at the same time.
2. When automatic migration is active, include the migration catalog in the CKFREEZE so that zSecure Admin and zSecure Audit know which data sets are migrated. Make sure you do not suppress the collection of these catalogs by specifying (`MCD=YES`, `DMS=YES`, or `ABR=YES`). In addition, make sure that zSecure Collect knows about the correct data set (`HSMMCD=`, `DMSFILES=`, or `ARCDSN=`).

   If a sensitive data set has been migrated, zSecure cannot get the PDS directory of the data set. For reliable analysis, recall the data set.
3. Include PDS directory dumps in a CKFREEZE data set so that zSecure Admin and zSecure Audit know what load modules are present in the PDSes. To ensure this, consider the following guidelines:
   a. To make sure PDS directories are dumped, run zSecure Collect with `FOCUS=AUDIT` or `FOCUS=RACF`.
   b. To automatically dump sensitive data sets such as APF and linklist libraries, run zSecure Collect APF-authorized.

      If zSecure Collect runs unauthorized, these sensitive data sets are not dumped automatically to avoid causing a large number of 913-38 abends. To override this default behavior, set `PDS=YES`. The user ID that runs the program must have READ access to the data sets.

c. To configure zSecure Collect to dump specific data sets, use PDSDIR=*dsname* statements. If the program does not run APF-authorized, you must ensure that the execution user ID has at least READ access to the data sets.

Note: It might be necessary to first resolve all conditions identified by VERIFY PROGRAM , for example, in case a data set moved to another volume.

VERIFY PROGRAM, PGM

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify that each data set/volume combination added as a member to a PROGRAM profile indeed refers to a valid partitioned data set. If the CKRCMD file has been allocated, commands are generated to remove the invalid data set/volume combinations from the PROGRAM profile.

If a VTOC or migration catalog that is required to decide whether there is a match is not found in the CKFREEZE file(s), the removal command is generated, but commented out. Messages in the SYSPRINT indicate why a certain decision was made. For more information about the messages, see *IBM Security zSecure: Messages Guide*. See VERIFY PGMEXIST for an explanation how to ensure all VTOCs are present for analysis.

Note: Running VERIFY PROGRAM might not be the only action needed to "fix" PROGRAM profile settings. You might have to manually add a new data set/volume combination to the profile if the data set was moved to another volume.

VERIFY PROTECTALL, PROT

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

VERIFY PROTECTALL verifies that all DASD data sets (including migrated data sets, as these will be recalled when allocating) are covered by at least one DATASET profile. In accordance with RACF, a generic profile is always considered sufficient (if the name matches), discrete profiles are only considered applicable to RACF-indicated data sets. An exception is made for ABR-migrated data sets, as the RACF-indicated flag can only be inspected by reading the migration tape. For these data sets, discrete profiles will be considered applicable if the ABR PROFKEEP option is active (which is unusual).

In a PROTECTALL(FAILURES) environment, data sets without a profile are inaccessible, in a NOPROTECTALL environment such data sets are unprotected. RACF-indicated data sets without discrete or matching generic profile are always inaccessible.

For RACF-indicated data sets without discrete or matching generic profile, an ADDSD command to create a discrete profile is generated. Note that most of the time this is not what you want; it is better to define a generic profile and PERMIT the groups requiring access. Generated commands are written to the CKRCMD file.

VERIFY SENSITIVE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•		

The VERIFY SENSITIVE command verifies the RACF-protection of system-sensitive data sets and generates RACF commands to adjust the protection. This command generates messages CKR0473 to CKR0485.

The VERIFY SENSITIVE is a companion to the sensitive data set report and the REPORT SENSITIVE command. The Sensitive data set report provides infomration on system-sensitive data sets. The REPORT SENSITIVE command reports on the RACF-protection of system-sensitive data sets.

Note: The sensitive data set report is also of use in non-RACF systems. The REPORT SENSITIVE and VERIFY SENSITIVE commands are not useful in non-RACF systems.

The VERIFY SENSITIVE command checks all RACF system-sensitive data sets to determine whether they are protected by a RACF profile, have the appropriate audit level defined or implied by LOGOPTIONS, SECLEVELAUDIT, or SECLABELAUDIT settings, and have the UACC and the access of ID '*' set at the appropriate level. If the protection is not adequate, commands are generated to update the protection. The generated commands update the RACF-protection in the following manner:

- Unprotected data sets are protected by a fully qualified generic profile with the appropriate UACC and audit options.
- Data sets inadequately protected by a fully qualified generic or discrete profile have their profile adjusted.
- Data sets inadequately protected by a generic profile get a new fully qualified generic profile, copied from the current generic profile. The new profile is then adjusted. In this manner, the access list, installation data, and other information from the old profile are preserved.

The VERIFY SENSITIVE command adheres to the CS-1 (Commercial Security 1) protection profile from the U.S. Federal Criteria and the Common Criteria V1.0 (currently a draft ISO standard). This is roughly equivalent to the C2 level of the orange book (see “SIMULATE” on page 911).

VERIFY STC

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

Verify the consistency of Started Procedure Table ICHRIN03 and the RACF STARTED class with the RACF user and group definitions, and with the procedure members of the JES2/JES3 and MSTR procedure libraries used for started tasks. The following conditions are flagged for ICHRIN03: non-startable procedures, procedures unable to use the user or group indicated by ICHRIN03, obsolete ICHRIN03 entries, protection deficiencies, hidden procedure members, and procedures running with the default RACF user '*' for various reasons. The following conditions are flagged for the RACF STARTED class: invalid or incomplete STARTED profiles; STARTED profiles not used by any procedure; procedures unable to use the correct STARTED profile and using user '++++++++'; procedures that do not match any STARTED profile and use ICHRIN03 instead. To

omit messages for the default user ID, add SUPPRESS ID=* or SUPPRESS ID=++++++++ [9] VERIFY STC is mutually exclusive with COPY, MOVE and REMOVE commands.

The following errors will be corrected or at least made more explicit if they occur on the profile level (that is, they are not the result of evaluating an =MEMBER specification for a started task matching a profile with a generic first qualifier): no STDATA segment, invalid STUSER, invalid STGROUP. For the first, an STDATA segment with an STUSER specification of =MEMBER will be generated if the first qualifier is a valid user ID, or NOUSER otherwise; invalid specifications will be either be corrected to =MEMBER or made more explicit by deleting them. The following errors will only be flagged: no connection between user and group, user ID revoked, errors on the member level. As much as possible, multiple error conditions are combined into one message, except that errors on the member level are not reported when an error message on the profile level is issued.

VERIFY TSOALLRACF

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•		

The VERIFY TSOALLRACF verifies that all users defined in the UADS data set are defined to RACF and have a TSO segment. It generates messages CKR0580 and CKR0581.

Users that are defined in the UADS data set, but not defined to RACF, are not subject to RACF password and revoke controls. Users that are defined in the UADS data set, are defined to RACF, but do not have a TSO segment, take their TSO attributes from the UADS data set. In both cases, the RACF administrator cannot properly control the TSO user.

Example - combining verifications

This example shows a combination of verification options that you could use for a periodical 'health-check' on your database.

```
verify program pads pgmexist protectall onvolume permit connect stc
```

Example - verifying started tasks

This example shows how to check the started task scene while suppressing messages for started tasks running with a default user ID.

```
verify stc
suppress id=*
```

9. If you have changed the JES undefined user from '++++++++' to something else, you should use the actual value on the suppress statement. This value is contained in the UNDEFINEDUSER field of NEWLIST TYPE=SYSTEM, which is reported in the SETROPTS report in “SETROPTS - RACF settings report” on page 266 under the heading "Job Entry Subsystem options" as "Default uid local UNDEFINEDU".

Chapter 13. SELECT/LIST Fields

This chapter provides information on the NEWLIST fields for selecting data and creating zSecure reports. Each NEWLIST type can be used to generate reports on a specific type of information. For example, the SYSTEM NEWLIST provides information about system-wide option settings. Each NEWLIST type has a set of fields that can be used in SELECT, EXCLUDE, and LIST statements for reporting about the specified information. For additional information on each NEWLIST type, associated fields, and usage notes, see the following sections.

ACCESS: Access Monitor Records

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•			

Use the NEWLIST TYPE=ACCESS for viewing and reporting on access information in the records collected by the zSecure Access Monitor. You can also use this NEWLIST to filter or summarize the information in the Access Monitor data sets.

The most common application is viewing and reporting on monitoring information. If you use the ACCESS NEWLIST to filter or summarize Access Monitor data sets, make sure that the output Access Monitor data set has the same layout and format as the input Access Monitor data set. For example, one of the requirements is to specify OPTION NULLS to avoid translating null (x'00) characters into blanks (x'40') in the output.

You can use most ACCESS NEWLIST fields for the following functions:

- Select and exclude information in a query with the SELECT and EXCLUDE commands.
- Generate output with the following output commands (LIST, SORTLIST, DISPLAY, and (D)SUMMARY.

Not all fields are available in all records. For example, many fields are not available on START and STOP records. If a field has restrictions, the restriction is noted in the field documentation. See "Field descriptions" on page 954.

The ACCESS NEWLIST supports two different formats of Access Monitor data sets. The first format is the one used in zSecure V1.12 and earlier releases. It is referred to as the V1.11 format. The second format is the one used in zSecure V1.13 and later releases. It is referenced to as the V1.13 format. Use of the V1.13 format allows use of the UNLOAD statement to perform fast consolidation of Access Monitor data sets. When using the UNLOAD statement to consolidate multiple Access Monitor data sets, all input data sets must be in V1.13 format. When not using an UNLOAD statement, a combination of V1.11 format and V1.13 format data sets can be used. Within a single NEWLIST, the UNLOAD statement cannot be combined with any other statement.

For more information about the Access Monitor data and the zSecure Access Monitor program, see Chapter 10, "RACF Access Monitor," on page 643.

Field descriptions

The ACCESS NEWLIST provides the following fields for reporting.

ACCESS_ALLOWED

Describes the allowed access. The value of the field depends on the RACROUTE REQUEST macro issued:

- For auth-type records (RECTYPE=AUTH), the ACCESS_ALLOWED field indicates the System Authorization Facility (SAF) access level allowed by RACF.
- For fastauth-type (RECTYPE=FAST) and define-type (RECTYPE=DEF) records, the ACCESS_ALLOWED field is not used and always has a value of *NONE*.

This field is not available for START and STOP records.

ACCESS_COUNT

Shows the number of RACROUTE requests of this type. The default format for this 32-bit number is UDEC, which might need up to 10 characters to show its value correctly. To accommodate narrower columns, the overriding output format UDEC$ABBR can be used. For numbers larger than 4 294 967 296, the field ACCESS_COUNT_BIG might be available. For creating V1.11 format Access Monitor records, use the ASIS output format. For creating V1.13 format Access Monitor records, use the ACCESS_COUNT_BIG field instead.

This field is not available in START and STOP records.

ACCESS_COUNT_BIG

Shows information similar to that shown for the ACCESS_COUNT field. The internal format of this field is a 64-bit number, which accommodates values up to 20 decimal digits. The default format for this 64-bit number is UDEC. If the number does not fit in the specified column width, asterisks are shown. To accommodate narrow columns the overriding format UDEC$ABBR can be used. For large numbers, the UDEC$ABBR format might also be easier to read. For creating V1.13 format Access Monitor data sets, use the ASIS output format.

This field is not available in START and STOP records.

ACCESS_FLAGS_RAW

This unformatted field contains bits that provide information about access request results, for example, a bit that indicates if an ACCESS_PROFILE is a generic or discrete profile. To display or report on this field, use the overriding format of (HEX,4).

This field is not available for START and STOP records. The ACCESS_FLAGS_RAW field summarizes the information that is provided in the individual ACCESS_* fields in the ACCESS NEWLIST in an unformatted bit field. To provide output in a more readable format, use the individual ACCESS_* fields to select and list the information instead of using this summary field.

ACCESS_GENERIC

This flag field (YES/NO) indicates whether the profile that was used to determine access privileges is generic or discrete. This field is not available for START and STOP records.

ACCESS_GLOBAL

This flag field (YES/NO) indicates whether the access request was granted using the global access checking (GAC) table. The ACCESS_GLOBAL value is based

on the actual processing by RACF. If an application requested a profile to be returned (reported by the "REQ_PRIVCSA" on page 959 flag), the ACCESS_GLOBAL flag value is NO.

This field is not available for START and STOP records.

ACCESS_IS_GROUP

This flag field (YES/NO) indicates if the userid used for the access request represents a RACF group. This situation occurs most often during access requests for DFP resources such as MGMTCLAS where access by the RESOWNER of the data set is checked. This field is not available for START and STOP records.

ACCESS_OPERATIONS

This flag field indicates that OPERATIONS authority, either group-OPERATIONS or system-wide OPERATIONS, was used to grant access. It is not possible to determine from this field if the RACF attribute was system-level or group-level. For DEFINE-type events, the field indicates whether OPERATIONS authority was used to define or delete a resource or profile. This field is set only if the RACF level supports it. For RACF releases that do not provide this data, Access Monitor records show a value of either No or missing depending on whether a CKFREEZE file was provided. See also "ATTRIB_OPERATIONS" on page 956.

ACCESS_PRIVTRUS

This flag field (YES/NO) indicates whether the address space issuing the access request has the Privileged or Trusted attribute. For RACROUTE REQUEST=AUTH macro requests (rectype=AUTH) issued from an address space that has either attribute (ACCESS_PRIVTRUS = YES), access is granted immediately without retrieving a profile. If the application also specifies that a profile be returned–reported by the "REQ_PRIVCSA" on page 959 field, then the privileged and trusted attributes are ignored by RACF.

Starting with z/OS 1.11, the privileged and trusted attributes are also honored by RACF and reported by the zSecure Access Monitor program for RACROUTE REQUEST=FASTAUTH macro requests (rectype=FAST).

The ACCESS_PRIVTRUS value is also reported for RACROUTE REQUEST=DEFINE(rectype=DEF) but is ignored by RACF. This field is not available for START and STOP records.

ACCESS_PROFILE

The profile name that was used for the resource specified in the RACROUTE call. When writing Access Monitor data sets, use the L1CHAR output format.

Although most auth-type and define-type records contain a profile name, the ACCESS_PROFILE field might be missing under certain conditions. Some aspects of this profile are output by the field "ACCESS_FLAGS" on page 954.

This field is not available in START and STOP records.

ACCESS_PROFTYPE

Indicates the type of profile that was used to grant or refuse the access. If no profile was used, the value returned can be either missing if there was no profile involved, or qualown if access was granted based on ownership of the resource key qualifier that determines ownership. For class DATASET, the value is the HLQ (High-level qualifier), which is the first qualifier as changed by any naming convention tables or exits.

Table 319. Access Profile Types for NEWLIST TYPE=ACCESS

Access profile type	Description
DISCRETE	Discrete general resource profile record.
GENERIC	Generic data set or general resource profile record.
GLOBAL	Global access table entry record.
missing	This value is returned when RACF did not use a profile for its decision, or if the profile could not be found.
MODEL	Model profile record.
NONVSAM	Discrete non-VSAM DATASET profile record.
TAPEDSN	Discrete tape data set profile record.
VSAM	Discrete VSAM profile.
qualown	Access granted based on ownership of the resource key qualifier that determines ownership. For the DATASET class, this value is the HLQ (High-level qualifier).

ACCESS_RESULT

Specifies the return code from the RACROUTE call, including the effects of PROTECTALL and the default return code for the class. For define-type records, the value is always zero even if the DELETE or DEFINE request is failed by RACF.

The ACCESS_RESULT field is not available for START and STOP records.

ACCESS_SPECIAL

This flag field indicates that SPECIAL authority was used to grant access. For example, the system-SPECIAL attribute might have been used to access a data set that has no RACF profile while PROTECTALL was active. For DEFINE-type events, the field indicates whether SPECIAL authority was used to define or delete a profile. This field is set only if the RACF level supports it. For RACF releases that do not provide this data, Access Monitor records show a value of either No or missing depending on whether a CKFREEZE file was provided. See also "ATTRIB_SPECIAL."

ACCESS_UNDEFINED_USER

This flag field (YES/NO) indicates whether the userid is RACF defined. This field is not available for START and STOP records.

ACCESS_USED_EXIT

This flag field indicates whether an installation exit was used to grant or deny the requested authorization. The field is present for AUTH and DEFINE records only, and is reported as missing for all other record types, including FAST. This field is set only if the RACF level supports it. For RACF releases that do not provide this data, Access Monitor records show a value of either No or missing depending on whether a CKFREEZE file was provided.

ATTRIB_OPERATIONS

This flag field indicates that the user's ACEE had the system-wide OPERATIONS bit set at the time of the access authorization. This value can reflect the attribute setting in the RACF database or reflect the temporary setting of the OPERATIONS bit by other programs to increase their authority.

ATTRIB_SPECIAL

This flag field indicates that the user's ACEE had the system-wide SPECIAL bit set at the time of the access authorization. This value can reflect the attribute setting in the RACF database or reflect the temporary setting of the OPERATIONS bit by other programs to increase their authority.

CLASS

Specifies the class name of the requested resource.

The field is not available for START and STOP records.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

Identifies the security complex of the system where this file originated. The value is derived from the system name in the SYSTEM field for the Access Monitor record, the `ALLOC COMPLEX=` specification for the Access Monitor file, and the systems and database allocations. The default field length is eight characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or zero. See "Modifying output length" on page 797.

DDNAME

Specifies the DDNAME of the $zsecures; ACCESS input file.

FLAGS_RAW

This is an unformatted field containing the flag bits that describe parameters on the RACROUTE request such as the RACFIND setting of a data set. To display and report on this field, use an override format of (HEX,2).

This field is not available for START and STOP records. For most applications, it is a good idea to use the individual REQ* fields instead of the FLAGS_RAW field.

INTENT

Describes the requested access. The value of the field depends on the RACROUTE REQUEST issued:

- For auth-type records (`RECTYPE=AUTH` and `RECTYPE=FAST`), the INTENT field value indicates the System Authorization Facility (SAF) access level requested. Possible values are READ, UPDATE, CONTROL and ALTER.
- For define-type records (`RECTYPE=DEF`), the value shows the type of DEFINE request. Possible values are `DEFCREA`, `DEFDELE`, `DEFCHGV` and `DEFADDV`.

The field is not available for START and STOP records.

INTENT_RAW

Describes the requested access in a one-byte bit-field. The value of the field depends on the RACROUTE REQUEST issued:

- For auth-type records (`RECTYPE=AUTH` and `RECTYPE=FAST`), the value represents the System Authorization Facility (SAF) access level requested.

- For define-type records (RECTYPE=DEF), the value represents the type of request: DEFINE, DELETE, ADDVOL, or CHNGVOL.

The field is not available for START and STOP records.

JOBNAME

Shows the name of the task where the access monitor event occurred. This field is reported as missing if the input record does not contain the field. For most ACCESS files, the JOBNAME field is present only for those userids for which the JOBNAME field has been activated in the C2PAMJOB customization member. The primary use of the JOBNAME field is with shared userids, such as those used in some job scheduling implementations, or those used for started tasks. For customizing the C2PAMJOB member, see Chapter 10, "RACF Access Monitor," on page 643.

LAST_TOD

The time of day (UTC) that the specific event last took place.

RECNO

Specifies the record number of the current record within its input file. The RECNO field applies to the number of complete logical records within a single input file, counting the first record as 1.

RECORD

Specifies the current record from the Access Monitor file. This field is mainly for debugging purposes.

RECORDLENGTH

Provides the length of the Access Monitor record in bytes, excluding the RDW, the first four bytes at the start of a variable record length file. The given length is the one of the logical record.

RECTYPE

Describes the type of record. Table 320 lists the possible values

Table 320. RECORD Types for NEWLIST TYPE=ACCESS

Value	Description
Start	START record marking start of interval.
Stop	STOP record marking end of interval.
Auth	AUTH - RACROUTE REQUEST=AUTH
Fast	FAST - RACROUTE REQUEST=FASTAUTH
Define	DEF - RACROUTE REQUEST=DEFINE

REQ_CHECKAUTH

This flag field (YES/NO) indicates whether the RACROUTE REQUEST=DEFINE macro requested that RACF perform an internal RACROUTE REQUEST=AUTH. This function is intended to be used by the RACF command processors.

This field is not available for AUTH, FAST, START, and STOP records.

REQ_COMMAND

This flag field (YES/NO) indicates whether the RACROUTE REQUEST=DEFINE macro is issued as the result of a RACF command.

This field is not available for AUTH, FAST, START, and STOP records.

REQ_GENERIC

This flag field (YES/NO) indicates whether the application that called the RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE macro explicitly requested that RACF considers the resource name as a generic profile name. This function is normally only used by the RACF command processors.

This field is not available for START and STOP records.

REQ_PRIVCSA

This flag field (YES/NO) indicates whether the application that called the RACROUTE REQUEST=AUTH macro requested that RACF return a profile in the Private area or in CSA. When this flag is set, RACF ignores the GAC table and the Privileged and Trusted attributes. For FAST records, the REQ_PRIVCSA value is NO.

This field is not available for DEF, START, and STOP records.

REQ_PROPAGATED

This flag field (YES/NO) indicates whether the RACROUTE REQUEST=DEFINE macro is issued as the result of an automatic direction of application updates.

This field is not available for AUTH, FAST, START, and STOP records.

REQ_RACFIND

This flag field (YES/NO) indicates the value specified by the application that called the RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE macro for the RACF Indicator. The flag field is missing if the application did not specify RACFIND.

This field is not available for START and STOP records.

REQ_RACFIND_SPECIFIED

This flag field (YES/NO) indicates whether the application that called the RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE macro specified that the resource has a RACF Indicator. If the application specified RACFIND, the REQ_RACFIND_SPECIFIED value is YES. If the application did not specify RACFIND, the value is NO. The value of the RACF Indicator is reported in the "REQ_RACFIND" field.

This field is not available for START and STOP records.

REQ_VERIFY

This flag field (YES/NO) indicates whether RACROUTE REQUEST=DEFINE macro verifies the user's authority only or whether it also defines a profile in the RACF database.

This field is not available for AUTH, FAST, START, and STOP records.

RESOURCE

Shows the SAF (System Authorization Facility) resource specified on the RACROUTE call. Most define-type records and some auth-type records contain a resource name. When writing Access Monitor data sets, you should use the L1CHAR output format.

This field is not available for START and STOP records.

SIM_CLASS

Indicates the class where the profile used is located. Possible values are: Grouping-Class, Member-Class or Class.

SIM_GENERIC

A flag to indicate that this is a generic profile. The default output length for the field is 3. The default format is Yes or No.

SIM_PROFILE

The name of the profile in SIM_CLASS that is used for access verification according to the current RACF database.

SIM_PROFTYPE

Type of profile in the current RACF database. The field output length is 8. For the meaning of the values, see the table with `TYPE=RACF_ACCESS` field `PROFTYPE`.

SIM_RESULT

A numeric field that indicates if the user has access based on the access list for the current RACF database. The reported result takes into account the effect of the RACF `PROTECTALL` setting. `SIM_RESULT` can have any of the following values:

8 indicates a violation

0 indicates success

4 indicates an undetermined status.

SYSTEM

The system id as mentioned in the Access Monitor file or stream.

USERID

The user id as mentioned in the Access Monitor file or stream.

This field is not available for `START` and `STOP` records.

UTOKEN_POE

This field shows the Port of Entry (POE) of the task where the Access Monitor event occurred. This field is reported as missing if the input record does not contain the field. For most ACCESS files, the UTOKEN_POE field is present only for those events for which POE processing has been activated in the C2PAMPCL and C2PAMRCL customization members. The primary use of the UTOKEN_POE field is with events, where access is granted using the conditional access list, such as for resources in the OPERCMDS class. For customizing the C2PAMJPCL and C2PAMRCL members, see Chapter 10, “RACF Access Monitor,” on page 643.

UTOKEN_POECLASS

Shows the CLASS of the Port of Entry of the task where the Access Monitor event occurred. This field is reported as missing if the input record does not contain the field. For most ACCESS files, the UTOKEN_POECLASS field is present only for those events for which POE processing has been activated in the C2PAMPCL and C2PAMRCL customization members. The primary use of the UTOKEN_POECLASS field is with events, where access is granted using the conditional access list, like for resources in the OPERCMDS class. For customizing the C2PAMJPCL and C2PAMRCL members, see Chapter 10, “RACF Access Monitor,” on page 643.

UTOKEN_POE_RAW

Shows the Port of Entry, concatenated to its CLASS, of the task where the Access Monitor event occurred. The CLASS is represented by its internal format. This field is primarily intended for consolidation of ACCESS files. It is present for only those events for which POE processing has been activated in the

C2PAMPCL and C2PAMRCL customization members. For customizing the C2PAMJPCL and C2PAMRCL members, see Chapter 10, “RACF Access Monitor,” on page 643.

AUDIT: System setting audit concerns

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

AUDIT NEWLIST type reports on the audit concerns raised by global option settings. Information about the global option settings is provided by the SYSTEM NEWLIST. The audit concerns reported might be affected by the SIMULATE POLICY setting.

Field descriptions

You can use the following fields to select and create audit reports for System settings.

AREA

The subsystem or area where this concern was detected MVS, SMF, HSM, DMS, SYSLOG, TSO, SETROPTS, and GSO. The default output length is 4, the actual field is 8 characters.

AREAPARM

Name of the setting or parameter within the AREA (as found in the PARMLIB or on the SETROPTS command). The field PARMNAME (when available) contains the name of the NEWLIST TYPE=SYSTEM CARLa field that describes the setting/parameter.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas.

The following audit concerns have been defined regarding common concerns in the MVS area:

- Security/integrity flaw remediation no longer guaranteed

  The z/OS release is no longer in service with IBM. Hence security or integrity exposures will no longer be fixed. You should upgrade to a more recent version to get the benefits of flaw remediation. The end-of-service date supplied by IBM for your operating system release level is compared against the date that the CKFREEZE file was made. If no CKFREEZE file is used, the current date is taken. The release level checked is available as field MVSLEVEL in the SYSTEM NEWLIST.
- Non-APF Refreshable modules can be modified despite Binder REFR setting

  The REFRPROT facility is available on this system but is set off. As a result, modules that are marked as Refreshable (not expected to be modified) can be modified by problem-state programs running in normal user key. This is both a RAS (Reliability/Availability/Serviceability) risk and a minor security risk.

The following audit concerns have been defined regarding common concerns in the VM area:

- Security/integrity flaw remediation no longer guaranteed

The VM or z/VM release is no longer in service with IBM. Hence security or integrity exposures are no longer fixed Upgrade to a more recent version to get the benefits of flaw remediation. The end-of-service date supplied by IBM for your operating system release level is compared against the date the CKFREEZE was made. If no CKFREEZE is used, the current date is taken.

The following audit concerns have been defined regarding common concerns in the HSM area:

- Disk scavenging threat not countered in HSM: *HSMNAME*/ not C2 compliant

  HSM is not erasing the disk when it deletes a data set from DASD after migration. This enables an attacker to allocate the disk space vacated and read the contents of the data set that has been migrated. This is a direct violation of the C2 security policy.

The following audit concerns have been defined regarding common concerns in the SMF area:

- No audit trail at all

  SMF collection is not active, hence the official operating system audit trail is not being written. This means that there is no user accountability for activities on the system.

- Hacker can work unobserved after flooding audit trail / not C2 compliant

  The security setting LASTDS(HALT) is not active. This setting should be active to operate on the C2 level defined in the Orange Book. Companies often value availability higher than other security measures and hence allow malicious users the opportunity to do their evil work without an audit trail. The flag is also available through the SMFLASTDSHALT field in the SYSTEM NEWLIST.

- Hacker can work unobserved after flooding audit buffers / not C2 compliant

  The security setting NOBUFFS(HALT) is not active. This setting should be active to operate on the C2 level defined in the Orange Book. Companies often value availability higher than other security measures and hence allow malicious users the opportunity to do their evil work without an audit trail. The flag is also available through field SMFNOBUFFSHALT in the SYSTEM NEWLIST.

The following audit concerns have been defined regarding common concerns in the SYSLOG area:

- Part of audit trail missing

  The SYSLOG is not active. Although the SMF data sets form the primary audit trail, the JES SYSLOG is also of value to be able to trace back what happened in the system, especially during startup processing. Also, in practice, the SYSLOG often contains messages for events even though the SMF logging was being suppressed. The flag is also available as field SYSLOG_ACTIVE in SYSTEM NEWLIST.

- Operator command parms and responses not in syslog

  Normally the system would contain the parameter HARDCOPY DEVNUM(SYSLOG) in the CONSOLxx PARMLIB member. This is however not the case, causing the SYSLOG to be incomplete. The flag is also available as field SYSLOG_COMMANDS in SYSTEM NEWLIST.

- Operator command parms and responses undetectable

  the system contains HARDCOPY CMDLEVEL(NOCMDS) in the CONSOLxxPARMLIB member. This causes operator commands, system commands, and there responses to be missing from the hardcopy log. The command level setting is available through the CON_HCPY_CMDLEVEL field in the SYSTEM NEWLIST.

The following audit concerns have been defined regarding common concerns in the TSO area:

- VTAM buffers are not confidential

  The TSO or VTAM buffers might contain confidential information like passwords. To erase this information after use, the CONFTXT option in PARMLIB member TSOKEYxx can be set. Currently it is not set. The flag is also available through the TSOCONFTXT field in the SYSTEM NEWLIST.

The following audit concerns have been defined regarding RACF concerns in the SETROPTS area:

- Profile changes in USER class are not audited

  Reflects the SETROPTS AUDIT(USER) setting. This audit concern indicates that profile changes in the USER class are not logged to SMF for the following commands: ADDUSER, ALTUSER, CONNECT, DELUSER, PASSWORD and REMOVE.

  These profile changes *are* logged when SPECIAL users execute the commands while the SETROPTS SAUDIT setting is active. In addition, some USER class profile changes are also logged when SETROPTS AUDIT(GROUP) is enabled.

- Profile changes in GROUP class are not audited

  This audit concern reflects the SETROPTS AUDIT(GROUP) setting. It indicates that profile changes in the GROUP class are not logged to SMF for the following commands: ADDGROUP, ALTGROUP, CONNECT, DELGROUP and REMOVE.

  These profile changes *are* logged when SPECIAL users execute the commands while the SETROPTS SAUDIT setting is active. In addition, some GROUP class profile changes are also logged when SETROPTS AUDIT(USER) is enabled.

- ADSP is inefficient

  Automatic Data Set Protection is an option to automatically add a discrete DATASET profile each time a data set is being created by a user that also has ADSP set in his user profile or the current connect group. This is an old-fashioned way of protecting data. The combination of PROTECTALL(FAIL) with generic DATASET profiles is easier to maintain. The flag is available through the SETRADSP field in the SYSTEM NEWLIST.

- Password to switch RACF database still at IBM default

  Any user with access to a console with command authority, or an APF utility that can issue commands, can switch the system to a different RACF database because the password for this operation is still set to the IBM default. The flag is available through the RVARYSWITCHPWSET field in the SYSTEM NEWLIST.

- Password to deactivate RACF still at IBM default

  Any user with access to a console with command authority, or an APF utility that can issue commands, can switch off RACF because the password to issue the RVARY STATUS command is still to the IBM default. This flag is available through the RVARYSTATUSPWSET field in the SYSTEM NEWLIST.

- Allowing unidentified batch work makes hacking easy / not C1 compliant

  The SETROPTS JES(NOBATCHALLRACF) setting for this system allows jobs to run without RACF identity and authentication, allowing access to resource according to global access table and UACC. This is a very dangerous setting because it allows hackers to run jobs on the system. These jobs can then be used to exploit other vulnerabilities like leaky SVCs which do not require any DATASET resource. This setting is also a direct violation of the requirements for a C1 rating according to the Orange Book. The flag is available through the BATCHALLRACF field in the SYSTEM NEWLIST.

- User with CLAUTH can bypass generic profiles / not B1 compliant

The SETROPTS NOGENERICOWNER setting for this system permits people with class authorization to circumvent generic profiles they do not have access on. They can do this by creating a more specific resource profile and giving themselves access through that profile. The GENERICOWNER setting was introduced to counter that risk, but it is not in use. This setting is also a direct violation of the requirements for a B1 rating according to the Orange Book. The setting is available through the GENERICOWNER field in the SYSTEM NEWLIST.

- Attempts to change protection not audited

  The SETROPTS NOCMDVIOL setting for this system causes security violations on RACF commands to be omitted from the audit trail. Unsuccessful attempts can be a sign of unauthorized attempts to tamper with the system, so should be audited. The setting is available through the CMDVIOL field in the SYSTEM NEWLIST.

- Apparently unused userids increase risk of hacking

  The SETROPTS NOINACTIVE setting for this system assures that user IDs remain usable even though they have not been used for years. Because any secret, a password for example, has a chance of being leaked that increases with time, this is a very dangerous setting. This is a real risk because you cannot be certain that all of the old RACF databases and backups were run with the ERASEONSCRATCH option for both disk and tape. If you want to investigate further, use the zSecure **AU.S** option to create reports that summarize how long valid user IDs have been unused and how old valid passwords are. Common settings for the NOINACTIVE parameter are in the 30 to 90 days range. Less safe systems have set it to 255. This setting is available through the INACTIVE field in the SYSTEM NEWLIST.

- Password risk increases with age

  The SETROPTS PASSWORD(NOINTERVAL) setting for this system assures that passwords remain valid for indefinite length. Since any secret (like a password) has a chance of being leaked that increases with time, this is a very dangerous setting. If you think you do not run that risk ask yourself what you do with old RACF databases and backups of RACF databases, do you really use erase-on-scratch on disk as well as tape? The AU.S category RACF USER contains reports that summarize how old your passwords are that can still be used for authentication, in case you want to investigate further. The most common setting for this parameter is in the 30 day range. Less safe systems have set it to 90 days or even 255. The setting is available as field INTERVAL in SYSTEM NEWLIST.

- Without MINCHANGE users can thwart the PWDHISTORY more easily

  This audit concern reflects the SETROPTS PASSWORD(MINCHANGE(0)) setting. It indicates that users can change their passwords more than once on the same day. Consequently, the user can clear his password history easily.

- Userid stealing by hackers undetectable

  The SETROPTS NOINITSTATS setting for this system means that the last use date of userids is not being maintained. This means that the users do not get a message at logon stating the last logon date and hence cannot identify (mis)use of their userid by others. The setting is available as field INITSTATS in SYSTEM NEWLIST.

- OPERATIONS activity undetectable

  The SETROPTS NOOPERAUDIT setting for this system means that no audit trail is written for activities by users that get access through their OPERATIONS or group-OPERATIONS attribute. Hence misuse of these userids can certainly not be detected. Statistics show most fraud is perpetrated by insiders.

Logging activity provides a deterrent against misuse. The setting is available as field OPERAUDIT in SYSTEM NEWLIST.

- Warnings do not prevent unauthorized access / not C2 compliant

  The SETROPTS PROTECTALL(WARNING) setting for this system means that access to data sets is granted by default. This setting is counter to any *protection by default* policy you might have. Some people mistakenly believe that this settings means *prevent access and warn*, but it means *allow access and warn*. This setting is also a direct violation of the requirements for a C2 rating according to the Orange Book. The parameter setting is available through the PROTECTALL field in the SYSTEM NEWLIST.

- The security system is not even called for each dataset / not C2 compliant

  The SETROPTS NOPROTECTALL setting for this system means that access to data sets is allowed by default. This is counter to any *protection by default* policy you might have. This setting is also a direct violation of the requirements for a C2 rating according to the Orange Book. The parameter setting is available as field PROTECTALL in SYSTEM NEWLIST.

- Disk scavenging threat not countered / not C2 compliant

  The SETROPTS NOERASE or ERASE setting for this system means that residual data in disk data sets is not cleared when they are deleted because the RACF DATASET profile does not have the ERASE flag enabled. As a result, sensitive data is accessible by arbitrary users through reallocation of the disk space. Some sites claim to have taken other countermeasures, namely forcing the data set to be empty at allocation. However, these countermeasures are typically limited to writing a file mark on the first track of the data sets and resetting the last block pointer. Although this operation gives the impression that the data set is empty when read with ISPF BROWSE for example, it does not prevent a program from accessing the other tracks in the data set and reading residual data from there. This setting is also a direct violation of the requirements for a C2 rating according to the Orange Book which requires that all data sets have the ERASE attribute. You can run the SETROPTS ERASE(ALL) command to set the attribute, but only after taking some performance measures to prepare your system for the new setting. As a rule of thumb, you must double the number of volumes mounted PUBLIC to cope with the doubling of the I/O load for temporary data sets. Also for systems with shared DASD, hardware catalog/VVDS reserves might require conversion to system-wide enqueues to prevent long catalog lockouts during VSAM data set erasure. The parameter setting is available through the ERASEONSCRATCH field in the SYSTEM NEWLIST.

- Security/integrity flaw remediation no longer guaranteed

  The operating system/RACF release is no longer in service with IBM. Hence security or integrity exposures will no longer be fixed. You should upgrade to a more recent version of the operating system to get the benefits of flaw remediation. The end-of-service date supplied by IBM for your operating system release level is compared separately against the dates that the CKFREEZE or UNLOAD were made. If no CKFREEZE is used, or a live database is used instead of an UNLOAD, the check is done against the current date. For a database copy the check is skipped. The release levels checked are available as fields MVSLEVEL and RACFLEVEL in NEWLIST TYPE=SYSTEM.

- Administrator activity undetectable

  The SETROPTS SAUDIT setting for this system means that no audit trail is written for activities by users that get access through their SPECIAL or group-SPECIAL attribute. Hence misuse of these userids can certainly not be

detected. Statistics show most fraud is perpetrated by insiders. Logging activity provides a deterrent against misuse. The setting is also available as field SAUDIT in NEWLIST TYPE=SYSTEM.

- Tape volumes are unprotected / not C1 compliant

  The SETROPTS NOTAPEDSN NOCLASSACT(TAPEVOL) setting for this system means that data on tape is not protected properly. This typically allows access to sensitive data through backup tapes. Even if you have a tape management system with extra protection measures, this usually is not sufficient. This setting is a direct violation of the requirements for a C1 rating according to the Orange Book. The parameter settings are available as fields TAPEDSN and TAPEVOL in NEWLIST TYPE=SYSTEM and field ACTIVE in NEWLIST TYPE=CLASS for CLASS=TAPEVOL.

- Tape data sets are unprotected unless TAPEVOL profiles exist.

  The SETROPTS NOTAPEDSN CLASSACT(TAPEVOL) setting for this system means that data on tape is only protected if TAPEVOL profiles exist. You should check that all backup tapes (typically containing sensitive data) are protected by a TAPEVOL profile, even if they are in scratch status (unless you want to erase them at expiry). The simplest way to accomplish proper protection is to have a separate pool for your backup tapes with a naming convention and a generic TAPEVOL profile with UACC(NONE) and permits for DASD management tasks, for example, B*.

  The parameter settings are available as field TAPEDSN and TAPEVOL in NEWLIST TYPE=SYSTEM and field ACTIVE in NEWLIST TYPE=CLASS for CLASS=TAPEVOL.

- Hacker can read/write any tape dataset by adding and backspacing / not C1 compliant

  The SETROPTS TAPEDSN NOCLASSACT(TAPEVOL) setting for this system means that data on tape is not protected properly. It is a widely spread misconception that tapes might be protectable by data set name only. Because a user might always create a data set with his own userid as high-level qualifier, he can add a data set to a tape that is not yet full, and gain access to the tape volume. Tape cartridge units do not have the equivalent of DASD extent checking, the hacker can then use file space backward commands to obtain access to the other data sets on tape. This attack can be countered by the SINGLEDSN or equivalent option in tape management systems, but usually we find this is not being used for backup tapes. The simplest way to accomplish proper protection is to have a separate pool for your backup tapes with a naming convention and a generic TAPEVOL profile with UACC(NONE) and permits for DASD management tasks, for example, B*. This setting is a direct violation of the requirements for a C1 rating according to the Orange Book.

  The parameter settings are available as field TAPEDSN and TAPEVOL in NEWLIST TYPE=SYSTEM and field ACTIVE in NEWLIST TYPE=CLASS for CLASS=TAPEVOL.

- Users can use same passwords over and over

  The SETROPTS PASSWORD(NOHISTORY) setting for this system allows users to keep the same password even though a password interval has been set. Since any secret (like a password) has a chance of being leaked that increases with time, this is a very dangerous setting. If you think you do not run that risk ask yourself what you do with old RACF databases and backups of RACF databases, do you really use erase-on-scratch on disk as well as tape? The setting is also available as field (PWD)HISTORY in NEWLIST TYPE=SYSTEM.

- Too many password violations allowed

  The SETROPTS PASSWORD(NOREVOKE) or PASSWORD(REVOKE(11)) or worse setting for this system allows hackers to do at least 10 password attempts per legitimate user logon (e.g. once a day) without a great chance of anybody noticing. This might well be sufficient to break into a system if the hacker knows the password rules. Common practice is to set REVOKE in the range 3 to 5, allow initial typing mistakes but preventing systematic guessing over a number of days. The setting is also available as field (PWD)REVOKE in NEWLIST TYPE=SYSTEM.
- SECLABEL integrity not guaranteed / not B1 compliant

  The SETROPTS NOSECLABELCONTROL setting for this system means that anybody with READ access to the security label might change profiles classified under that security label. Hence integrity of the label is not guaranteed. This setting is also a direct violation of the requirements for a B1 rating according to the Orange Book. The parameter setting is available as field SECLABELCONTROL in NEWLIST TYPE=SYSTEM.
- SECLABELs not required / not B1 compliant

  The SETROPTS NOMLACTIVE or MLACTIVE(WARNING) setting for this system allows access to data without security labels being required. This means that there is no Mandatory Access Control active. This setting is a direct violation of the requirements for a B1 rating according to the Orange Book. The parameter setting is available as field MLACTIVE in NEWLIST TYPE=SYSTEM.
- Users can declassify data / not B1 compliant

  The SETROPTS NOMLS or MLS(WARNING) setting for this system allows users to declassify data. This means that there is no Mandatory Access Control enforced. This setting is a direct violation of the requirements for a B1 rating according to the Orange Book. The parameter setting is available as field MLS in NEWLIST TYPE=SYSTEM.
- SECLABEL meaning not stabilized / not B1 compliant

  The SETROPTS NOMLSTABLE setting for this system means that the meaning of a security label in terms of security categories and security level might be changed. This means that there is no Mandatory Access Control enforced. This setting is a direct violation of the requirements for a B1 rating according to the Orange Book. The parameter setting is available as field MLSTABLE in NEWLIST TYPE=SYSTEM.
- Uncataloged dataset not B1 audited / not B1 compliant

  The SETROPTS NOCATDSNS or SETROPTS CATDSNS(WARNING) setting for this system means that uncataloged data sets, including temporary data sets, are accessible to normal users without the proper audit trails being written. This setting is a direct violation of the requirements for a B1 rating according to the Orange Book. The parameter setting is available as field CATDSNS in NEWLIST TYPE=SYSTEM.

The following audit concerns have been defined regarding RACF concerns in the DMS area:

- DMS ignores RACF

  The RACFPROCN setting for this system means that DMS does not consult RACF when processing RACF indicated data sets. This allows access to other people's data through DMS. The parameter setting is available as field DMSRACFPROC in NEWLIST TYPE=SYSTEM.
- DMS will not backup RACF protected data

The RACFSUPPN setting for this system means that DMS does backup or restore any RACF-indicated data sets. This might be a serious risk for availability. The parameter setting is available as field DMSRACFSUPP in NEWLIST TYPE=SYSTEM.

- DMS ignores RACF for non-indicated data

  The RACFALWZN setting for this system means that DMS does not consult RACF when processing non-RACF-indicated data sets (usually the majority of data sets). This allows access to other people's data through DMS. The parameter setting is available as field DMSRACFALWZ in NEWLIST TYPE=SYSTEM.

- DMS restore to newname does not check RACF authority

  The RACFNEWNY setting for this system means that DMS does not consult RACF with the old name when renaming data sets during a restore. This allows access to other people's data though DMS by restoring their data set with a new name that you do have access to. This dangerous parameter setting has been found many times during security reviews. The parameter setting is available as field DMSRACFNEWN in NEWLIST TYPE=SYSTEM.

- DMS parameter override not secured

  The absence of the SECURE_PARMLIB flag in the load module ADSTS148 for this system means that DMS does not prevent a user from calling DMS with an alternate parameter library, opening up all other holes documented here for the DMS area. This allows access to other people's data. This dangerous parameter setting has been found many times during security reviews. The parameter setting is available as field DMS_SECURE_PARMLIB in NEWLIST TYPE=SYSTEM.

- DMS does not use DASDVOL, this is inefficient

  The SECURVOLN setting for this system means that DMS does not check the DASDVOL class first. While this is normal for systems with mandatory Access Control (B1), it is much more efficient for daily backups in RACF systems that are to run C2 or lower. The parameter setting is available as field DMSSECURVOL in NEWLIST TYPE=SYSTEM.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 321. AUDIT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This fields returns the complex name for the system where the audit concern was detected. The default output length is 8 characters.

PARMNAME

Name of the NEWLIST TYPE=SYSTEM CARLa field that contains the setting/parameter that caused the audit concern. The field AREAPARM contains the name of the system setting/parameter as found e.g. in the PARMLIB or on the SETROPTS command.

This field can be empty when the audit concern does not (directly) apply to a NEWLIST TYPE=SYSTEM field. The PARMNAME field can be used for generating NEWLIST TYPE=SYSTEM queries.

PARMVALUE

Value of the parameter listed in field PARMNAME that caused this audit concern. This is always a character value, even if in NEWLIST TYPE=SYSTEM the parameter is not a character value. The default output length is 8 characters.

SYSTEM

The name of the system where the audit concern was detected (SMF id for MVS systems). The default output length is 8.

AUTAB: RACF Authorized Caller Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The AUTAB NEWLIST (NEWLIST TYPE=AUTAB) displays the Authorized Caller Table. This NEWLIST generates one entry for each entry in the table. A unique key is SYSTEM ORDER. Unless otherwise stated, all fields can be used for SELECT or EXCLUDE processing as well as in the output commands (LIST, SORTLIST, DISPLAY and SUMMARY).

Field descriptions

You can use the following fields to select and create audit reports for the RACF Authorized Caller Table.

ATTR, AUTH

A string containing the program's authorization. If the RACLIST flag is set (RACLIST=YES), this string contains 'RACLIST'; if the RACINIT flag is set (RACINIT=YES), this string contains 'RACINIT'; if both are set, it contains 'RACLIST RACINIT'.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

ORDER, ORG

The original order (entry number) of this program in the authorized caller table. The first entry in the table has ORDER=1.

PROGRAM

The name of the program. This program must reside in an APF-authorized library.

RACINIT

RACINIT flag. A program that has this flag set (RACINIT=YES) is authorized to issue RACINIT requests, which perform user and potentially password verification.

RACLIST

RACLIST flag. A program that has this flag set (RACLIST=YES) is authorized to issue RACLIST requests, which load profiles into the main in-storage.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters to cater to VM systems.

CICS_PROGRAM: CICS programs

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

This section documents the fields for the NEWLIST TYPE=CICS_PROGRAM. This NEWLIST type lists one entry per active CICS program for a CICS region in each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, JOBNAME, and PROGRAM.

Field descriptions

The `CICS_PROGRAM NEWLIST` provides the following fields for reporting.

API_SUBSET

This field specifies whether the CICS program is restricted to a data program link (DPL) subset of the CICS API commands. Field value: Yes or No. If the value is Yes, the program cannot issue the following commands:

- Terminal control commands that reference the principal facility.
- Options of ASSIGN that return terminal attributes.
- BMS commands.
- Signon and signoff commands.
- Batch data interchange commands.
- Commands that address the TCTUA.

ASID

This field contains the address space ID associated with the CICS region. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 322. CICS_PROGRAM NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CEDF

This field specifies the action taken by the execution diagnostic facility (EDF) when the CICS program is running under EDF control. If the value is Yes, the EDF diagnostic screens are displayed. Field value: Yes or No.

CLASS

This field specifies the resource class used to secure the CICS program, for example, the MCICSPPT resource class. Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

DATA_KEY

This field specifies whether the storage that CICS allocates at task initialization is obtained from CICS-key or user-key storage. If the value is Yes, storage is obtained from user-key storage. If the value is No, storage is obtained from CICS-key storage. Field value: Yes or No.

DATA_LOCATION

This field specifies whether the data returned by commands using the SET option can be located above the 16 MB line. If the value is No, the data returned is located below the 16 MB line. Field value: Yes or No.

ENABLED

This field specifies the program status. If the value is Yes, the program can be executed normally. If the value is No, the program is disabled and cannot be executed. Field value: Yes or No.

JOBID

This field contains the JES job ID of the CICS region. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the CICS region. Maximum length: 8 characters.

JVM

This field specifies whether the program is a Java program that has to run in a Java Virtual Machine (JVM) in a CICS region. Field value: Yes or No.

JVMCLASS

This field specifies the fully-qualified name of the main class in a Java program. The fully-qualified name *package_name.class_name* is the class name qualified by the package name. For example, HelloWorld.HelloCICSWorld. Maximum length: 255 characters.

JVMPROF

This field specifies the name of a JVM profile, a file in the z/OS UNIX directory that is specified by the JVMPROFILEDIR system initialization parameter. Maximum length: 8 characters.

LANG_DED

This field specifies the program language that was deduced by CICS for the program.

LANG_DEF

This field specifies the programming language defined on the resource definition.

OPENAPI_DED

This field specifies if the program is restricted (Yes) to the CICS API or not (No). This value is deduced by CICS for the program. Field value: Yes or No.

OPENAPI_DEF

This field specifies if the program is restricted (Yes) to the CICS API or not (No). This value is the API attribute of the installed program definition.

PGM_TYPE

This field shows the CICS program type. Field values: PROGRAM, MAPSET, and PARTITIONSET.

PROGRAM

This field specifies the name of the CICS program. Maximum length: 8 characters.

QUALIFIED_RESOURCE

This field specifies the qualified resource name. The name is the concatenation of the RESOURCE_LOCATION and the RESOURCE separated by a colon, for example: IPO1.CICS.CICSTS41.PGM:CICSSTC.DFHEMTP. Maximum length: 48 characters.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE. You can use the UNIVERSAL modifier to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_CLASS

This field contains the resource class of the profile that protects the resource. The resource class can be a member class or a grouping class. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 8 characters.

RACF_PROFILE

This field contains the name of the profile that protects the resource. The profile can be a member class profile or a grouping class profile. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 8 characters.

RACF_UACC

This field contains the effective universal access authority (UACC) to the program. The UACC is determined from all grouping and non-grouping resource profiles that describe the program. Field values: NONE, READ, EXECUTE, UPDATE, CONTROL, or ALTER.

RELOAD

This field specifies whether a program control LINK, LOAD, or XCTL request reloads a new copy of a previously loaded program. If the value is No, any valid copy of the program currently in storage is reused for the request. If the value is Yes, a new copy of the program is loaded into storage for every program control request. This attribute does not apply to Java programs. Field value: Yes or No.

RESIDENT

This field specifies the resident status of the program. This attribute does not apply to JVM programs. If the value is Yes, the program is loaded on first reference and is permanently resident in virtual storage, but is to be pageable by the operating system. Field value: Yes or No.

RESOURCE

This field specifies the name of the resource that is used to secure the CICS program. Maximum length: 246 characters. Default length: 17 characters.

RESOURCE_LOCATION

This field indicates the environment where the resource is relevant. This field is the concatenation of several fixed strings, fields, and lookups, such as *system*.CICS.*jobname*.PGM. An example value of this format is IPO1.CICS.CICSTS41.PGM. Maximum length: 30 characters.

RMT_DYNAMIC

This field specifies whether the request to execute the CICS program can be dynamically routed. If the value is Yes, the CICS dynamic routing program is invoked. Field value: Yes or No.

RMT_NAME

This field specifies the name by which the CICS program is known in the remote CICS region, specified by the RMT_SYSTEM field. Maximum length: 8 characters.

RMT_SYSTEM

The field specifies the name of a remote CICS region to which a CICS client region ships a program link (DPL) request. Maximum length: 8 characters.

RMT_TRANSID

This field specifies the name of the transaction that the remote CICS server program attaches to and under which it runs the remote application program. Maximum length: 8 characters.

STEPNAME

This field contains the step name associated with the CICS region. Maximum length: 8 characters.

SYSIDNT

This field specifies a 1-to 4-character name to identify your local CICS region.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

THREADSAFE_DED

This field shows the threadsafe standard setting that is deduced by CICS for the program. If the value is Yes, the program is written to threadsafe standards. Field value: Yes or No.

THREADSAFE_DEF

This field indicates the threadsafe standard setting defined for the CICS program. If the value is Yes, the program is written to threadsafe standards. Field value: Yes or No.

VTAM_APPLID

This field specifies the specific VTAM application identifier (APPLID) for the CICS region. Maximum length: 8 characters.

CICS_REGION: CICS regions

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•		•	•	•	•	•

This section documents the fields for the NEWLIST TYPE=CICS_REGION. This NEWLIST type lists one entry per active CICS region for each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, and JOBNAME.

Field descriptions

The CICS_REGION NEWLIST provides the following fields for reporting.

AI_CONSOLE

This field identifies whether autoinstall status for consoles is active. Field value: Yes or No.

AI_EXIT

This field contains the name of the autoinstall exit control program for console autoinstall. Maximum length: 8 characters.

ASID

This field contains the address space ID associated with the CICS region. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 323. CICS_REGION NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CICS_LEVEL

This field identifies the CICS system release level of the active CICS region.

CLASS_APPC

This field specifies the resource class used to perform APPC session security. This resource class is used to determine access permission when SEC_APPC=YES. The field is empty when SEC_APPC=NO. Maximum length: 8 characters.

CLASS_CMD

This field specifies the resource class used to secure CICS commands. This resource class is used to determine access permission when SEC_CMD=YES and

command checking is active for the transaction. The field is empty when SEC_CMD=NO. Maximum length: 8 characters.

CLASS_DB2

This field specifies the CICS resource class used to secure the DB2ENTRY resources. This class is used to determine access permission when SEC_DB2=YES. The field is empty when SEC_DB2=NO. Maximum length: 8 characters.

CLASS_DCT

This field specifies the resource class used to secure the CICS transient data. This resource class is used to determine access permission when SEC_DCT=YES and resource checking is active for the transaction. The field is empty when SEC_DCT=NO. Maximum length: 8 characters.

CLASS_EJB

This field specifies the CICS resource class used to secure the EJBROLE resources. This resource class is used to determine access permission when SEC_EJB=YES. The field is empty when SEC_EJB=NO. Maximum length: 8 characters.

CLASS_FCT

This field specifies the CICS resource class used to secure the CICS files. This resource class is used to determine access permission when SEC_FCT=YES and resource checking is active for the transaction. The field is empty when SEC_FCT=NO. Maximum length: 8 characters.

CLASS_JCT

This field specifies the CICS resource class used to secure the CICS journals. This resource class is used to determine access permission when SEC_JCT=YES and resource checking is active for the transaction. The field is empty when SEC_JCT=NO. Maximum length: 8 characters.

CLASS_PCT

This field specifies the CICS resource class used to secure the CICS-started transactions. This resource class is used to determine access permission when SEC_PCT=YES. The field is empty when SEC_PCT=NO. Maximum length: 8 characters.

CLASS_PPT

This field specifies the CICS resource class used to secure the CICS programs. This resource class is used to determine access permission when SEC_PCT=YES and resource checking is active for the transaction. The field is missing when SEC_PCT=NO. Maximum length: 8 characters.

CLASS_PSB

This field specifies the CICS resource class used to secure PSB schedule requests in the CICS region. This resource class is used to determine access permission when SEC_PSB=YES and resource checking is active for the transaction. The field is empty when SEC_PSB=NO. Maximum length: 8 characters.

CLASS_RES

This field specifies the CICS resource class used to secure the general CICS resources. This resource class is used to determine access permission when SEC_RES=YES and resource checking is active for the transaction. The field is empty when SEC_RES=NO. Maximum length: 8 characters.

CLASS_SUR

This field specifies the CICS resource class used to determine if a CICS region user ID has authorization to act as a surrogate user. This resource class is used when SEC_SUR=YES. The field is empty when SEC_SUR=NO. Maximum length: 8 characters.

CLASS_TRN

This field specifies the CICS resource class used to secure the attached transactions. This resource class is used to determine access when SEC_TRN=YES. The field is empty when SEC_TRN=NO. Maximum length: 8 characters.

CLASS_TST

This field specifies the CICS resource class used to secure the CICS temporary storage queues. This resource class is used to determine access when the following conditions exist: SEC_TST=YES, resource checking is active for the transaction, and the temporary storage queue has been defined with TYPE=SECURITY. This field is empty when SEC_TST=NO. Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

CSD_DISP

This field contains the disposition of the CICS system definition (CSD) data set. A value of OLD means that the data set is used exclusively by the CICS region. A value of SHR means that the data set can be shared with other users or jobs.

CSD_DSN

This field contains the name of the CICS system definition (CSD) data set. The CSD file is a VSAM data set that contains a resource definition record for every resource defined to CICS by means of the CEDA transaction or the DFHCSDUP utility program.

CSD_READONLY

This field determines whether the CICS system definition (CSD) data set in use by the CICS region is set for read-only access. A value of Yes means that the data set cannot be updated by using the CEDA and CEDB transactions.

DEFAULT_USER

This field contains the default user id associated with the CICS region.

DLI_PSBCHK

This field determines whether a security check for remote users is performed at PSB schedule time. Field value: Yes or No.

EJBROLE_PREFIX

This field specifies the prefix that is used to qualify the security role defined in the deployment descriptor of an enterprise bean. Maximum length: 16 characters. The prefix is applied to the security role when:

- a role is defined to an external security manager
- CICS maps a security role to a RACF user ID
- an application invokes the `isCallerInRole()` method

GMTEXT

This field contains the default text that is displayed by the good morning or CSGM transaction. Maximum length: 246 characters.

GMTRAN

This field contains the CICS transaction that is invoked when a user logs on to the CICS region. If the field value is CSGM, the text in the GMTEXT field is displayed. Maximum length: 4 characters.

GNTRAN

This field specifies the good night transaction that CICS invokes upon expiration of a user's terminal timeout period. If set to the default value of GNTRAN=NO, CICS attempts to sign off the terminal user instead of invoking the good night transaction. The success of the signoff attempt depends on the value of the SIGNOFF attribute of the terminal's TYPETERM definition. Maximum length: 4 characters.

GRPLIST

This field is a repeat group which specifies the resource groups that contain the resource definitions required by the CICS region and that are installed as a part of CICS initialization. Resource groups can be either specific or generic. A maximum of four resource groups can be specified. Maximum length: 8 characters.

HPO

This field reports whether the MVS high-performance option (HPO) is active. If HPO=Yes, HPO is used improve user performance by reducing the transaction pathlength for processing VTAM requests. Field value: Yes or No.

HPO_SVCNO

This field specifies the Type 6 SVC number that is used by CICS to improve performance by reducing the transaction pathlength through VTAM.

JOBID

This field might contain the JES job ID of the CICS region. Maximum length: 8 characters.

JOBNAME

This field might contain the JES job name of the CICS region. Maximum length: 8 characters.

KEYRING

This field specifies the fully-qualified, case-sensitive name of the key ring file that is stored in an external security manager database. The key ring contains the keys and X.509 certificates that are used by CICS to support secure sockets layer (SSL) and Web services security. Maximum length: 47 characters.

PGM_LLACOPY

This field specifies whether CICS issues an LLACOPY macro each time a module is located from the RPL data set. Field values: Yes, No, or New.

PGM_LLACOPY=Yes
CICS issues the LLACOPY macro either on the first ACQUIRE or on any subsequent NEWCOPY or PHASEIN requests. This ensures that CICS always obtains the latest copy of any LLA-managed modules.

PGM_LLACOPY=No
CICS never issues an LLACOPY macro. Instead, each time the RPL data set is searched for a module, a BLDL macro is issued.

PGM_LLACOPY=New
CICS issues the LLACOPY macro when loading a module as a result of a NEWCOPY or PHASEIN request. A BLDL macro is issued for all other requests.

PGM_LPA

This field specifies whether load modules are loaded from the link pack area (LPA). Field value: Yes or No.

PGM_PRVMOD

This field is a repeated field that lists the modules that the CICS region cannot use from the MVS link pack area (LPA). Each repeated entry has a length of 8 characters. Maximum length: 8 characters.

PGM_RENTPGM

This field specifies whether CICS uses read-only, key-0 protected storage for re-entrant programs (PGM_RENTPGM=Yes). For CICS production regions, a setting of PGM_RENTPGM=Yes is commonly used, and for CICS development regions, a setting of PGM_RENTPGM=No is commonly used. Field value: Yes or No.

PLTPI_SEC

This field specifies whether CICS performs command security or resource security checking for PLT programs during CICS initialization. PLT programs run under the authority of the userid specified on PLTPI_USER, this userid must be authorized to access resources defined by the CICS PLTPISEC parameter. Field values: None, Cmdsec, Ressec, or All.

PLTPI_USER

This field specifies the userid that CICS uses for security checking for PLT programs that run during CICS initialization. All PLT programs run under the authority of this userid so it must be authorized to all the resources referenced by PLT programs, as defined by the CICS PLTPISEC parameter.

REGION_USER

This field specifies the userid that is associated with the CICS region. It is the default userid for the SEC_PREFIX if resource prefixing is requested, but no specific userid was specified, and it is also the userid that must be authorized to access CICS category 1 transactions. Maximum length: 8 characters.

SEC_APPC

This field shows whether the SESSION segment for the profiles in the APPCLU class are used during the verification of APPC BIND security when binding APPC sessions. Field value: Yes or No.

SEC_CMD

This field specifies whether command security checking is performed for the CICS region. A transaction definition controls whether command security checking is performed for an individual transaction. Field value: Yes or No.

SEC_CMDSEC

This field specifies whether command security checking is always performed for the CICS region independent of security checking required by transaction definitions. Field value: Yes or No.

SEC_DB2

This field specifies whether DB2 resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_DB2 is used to check whether the userid associated with the CICS DB2 transaction has access to the DB2ENTRY referenced by the transaction. Field value: Yes or No.

SEC_DCT

This field specifies whether transient data resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_DCT is used to check whether the userid associated with the CICS transaction has access to the specified transient data. Field value: Yes or No.

SEC_EJB

This field specifies whether CICS support for security roles is enabled. If the value is Yes:

- When an application invokes a method of an enterprise bean, CICS calls the external security manager to verify that the userid associated with the transaction is defined in at least one of the security roles associated with the method.
- When an application invokes the isCallerInRole() method, CICS calls the external security manager to determine whether the userid associated with the transaction is defined in the role specified on the method call.

Field value: Yes or No

SEC_ESM

This field specifies whether CICS resource security checking is performed for the CICS region by an external security manager, for example, RACF. Field value: Yes or No.

SEC_FCT

This field specifies whether file resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_FCT is used to check whether the userid associated with the CICS transaction has access to the specified file. Field value: Yes or No.

SEC_JCT

This field specifies whether journal resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_JCT is used to check whether the userid associated with the CICS transaction has access to the specified journal. Field value: Yes or No.

SEC_PCT

This field specifies whether resource security checking for started transactions is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_PCT is used to check whether the userid associated with the CICS transaction has access to the specified transaction. Field value: Yes or No.

SEC_PPT

This field specifies whether resource security checking of application programs is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_PPT is used to check whether the userid associated with the CICS transaction is authorized to use LINK, LOAD, or XCTL commands to invoke other programs. Field value: Yes or No.

SEC_PREFIX

This field specifies the string used to prefix all SAF resource names. It is alphanumeric and must start with an alphabetic character. This field is empty if prefixing is not used for this CICS region. Maximum length: 8 characters.

SEC_PSB

This field specifies whether program specification block (PSB) resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_PSB is used to check whether the userid associated with the CICS transaction is authorized to access the IMS PSB. Field value: Yes or No.

SEC_RES

This field specifies whether resource security checking is performed for the CICS region. A transaction definition controls whether command security checking is performed for an individual transaction. Field value: Yes or No.

SEC_RESSEC

This field specifies whether resource security checking is always performed for the CICS region independent of security checking required by individual transaction definitions. Field value: Yes or No.

SEC_SUR

This field specifies whether surrogate user resource security checking is performed for the CICS region. If the value is Yes, the general resource class specified in CLASS_SUR is used to check whether the CICS region userid has authorization to act as a surrogate. Field value: Yes or No.

SEC_TRN

This field specifies whether security checking is done to determine a user's authority to execute a transaction. If the value is Yes, the resource class specified in CLASS_TRN is used to check whether the userid associated with the CICS transaction has access to the transaction. Field value: Yes or No.

SEC_TST

This field specifies whether temporary storage resource security checking is performed for the CICS region. If the value is Yes, the general resource class

specified in CLASS_TST might be used to check whether the userid associated with the CICS transaction has access to the specified temporary storage queue. Field value: Yes or No.

SEC_UNIXFILE

This field specifies whether UNIX file security checking is performed for the CICS region. If the value is Yes, then z/OS UNIX system services controls access to the z/OS UNIX files and access is not managed directly by RACF. Field value: Yes or No.

SSL_ENCRYPT

This field specifies whether Secure Sockets Layer (SSL) is used for encrypting transmitted data. Field value: Yes or No.

STEPNAME

This field contains the step name associated with the CICS region. Maximum length: 8 characters.

STOR_CMDPROT

This field specifies whether CICS validates the start addresses of storage that is referenced as output parameters on EXEC CICS commands. If the value is Yes, CICS validates the start address to ensure that the application program has write access. If an application program asks CICS to write to an area where it does not have addressability, CICS abends the task with an AEYD abend. Field value: Yes or No.

STOR_CWAKEY

This field specifies whether CICS obtains storage for the common work area (CWA) in the CICS-key storage. If the value is Yes, storage is obtained in the CICS-key storage, otherwise it is obtained from the user-key storage. Field value: Yes or No.

STOR_PROT

This field specifies whether storage protection is used in the CICS region. If the value is Yes, CICS operates with storage protection and observes the storage keys and execution keys used in various system and resource definitions. Field value: Yes or No.

STOR_TASKCHK

This field specifies whether the task storage-violation checking at startup is activated or deactivated. Field value: Yes or No.

STOR_TCTUAKEY

This field specifies whether CICS obtains storage for the terminal user areas (TCTUA) in the CICS key storage. If the value is Yes, then storage is obtained in the CICS-key storage otherwise it is obtained from the user-key storage. Field value: Yes or No.

STOR_TCTUALOC

This field specifies where terminal user areas (TCTUA) are to be stored. If the value is Yes, the TCTUA is stored in virtual storage above the 16 MB line. Field value: Yes or No.

STOR_TERMCHK

This field specifies whether the terminal storage-violation checking is activated or deactivated. If the value is Yes, TIOA storage violations are checked. Field value: Yes or No.

STOR_TRANISO

This field and the STOR_PROT parameter specify whether transaction isolation is active in the CICS region. If STOR_TRANISO=Yes and STOR_PROT=Yes, CICS operates with transaction isolation. Transaction isolation ensures that only user-key programs of transactions defined with ISOLATE(YES) have access to the user-key task-lifetime storage of their own task. Field value: Yes or No.

SVCNO

This field specifies the Type 3 SVC number that is used by the CICS region.

SYSIDNT

This field specifies a 1-to 4-character name to identify your local CICS region.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

TRACE_CONFDATA

This field specifies whether CICS shows all user data that might otherwise appear only in CICS trace entries or in dumps that contain the VTAM receive any input area (RAIA). Field value: Yes or No.

TRACE_CONFTXT

This field specifies whether CICS allows VTAM to trace user data. Field value: Yes or No.

VTAM_APPLID

This field specifies the specific VTAM application identifier (APPLID) for the CICS region. Maximum length: 8 characters.

VTAM_GENAPPLID

This field specifies the generic VTAM application identifier (APPLID) for the CICS region. Maximum length: 8 characters.

VTAM_GRNAME

This field specifies the VTAM generic resource name used by a group of terminal-owning regions in a CICSplex to register to VTAM. Maximum length: 8 characters.

CICS_TRANSACTION: CICS transactions

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

This section documents the fields for the NEWLIST TYPE=CICS_TRANSACTION. This NEWLIST type lists one entry per active CICS transaction for a CICS region in each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, JOBNAME. and TRANSACTION.

Field descriptions

The CICS_TRANSACTION NEWLIST provides the following fields for reporting.

ASID

This field contains the address space ID associated with the CICS region. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 324. CICS_TRANSACTION NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CLASS

This field specifies the resource class used to secure the CICS program, for example, TCICSTRN. Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

DATA_CLEAR

This field specifies whether task-lifetime storage for the transaction is to be cleared on transaction release. Releasing the storage prevents other tasks from accidently viewing data stored by this transaction in task-lifetime storage. Field value: Yes or No.

DATA_FREEZE

This field specifies whether the storage for the transaction is retained for the duration of the transaction. Field value: Yes or No.

DATA_KEY

This field specifies whether the storage that CICS allocates at task initialization is obtained from CICS-key or user-key storage. If the value is Yes, storage is obtained from user-key storage. If the value is No, storage is obtained from CICS-key storage. Field value: Yes or No.

DATA_LOCATION

This field specifies whether task life-time storage acquired by CICS for the transaction duration can be located above the 16 MB line in virtual storage. If the value is No, CICS acquires data storage located below the 16 MB line. Field value: Yes or No.

ENABLED

This field specifies the transaction status. If the value is Yes, the transaction is enabled and can be executed normally. If the value is No, the transaction is disabled and cannot be executed. Field value: Yes or No.

JOBID

This field contains the JES job ID of the CICS region. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the CICS region. Maximum length: 8 characters.

OTS_TIMEOUT

This field specifies the a time (in hours, minutes, and seconds) that an enterprise bean Object Transaction Service (OTS) transaction, executing as a task under a CICS transaction, is allowed to execute before the initiator of the OTS transaction takes a syncpoint or rolls back the transaction. If the time period expires, CICS purges the task.

PRIORITY

This field specifies the transaction priority as a 1- to 3-digit decimal value from 0 to 255. This value is used to establish the overall transaction processing priority.

PROGRAM

This field specifies the name of the program to which CICS gives control in order to process this transaction. Maximum length: 8 characters.

QUALIFIED_RESOURCE

This field specifies the qualified resource name. The name is the concatenation of the RESOURCE_LOCATION and the RESOURCE separated by a colon, for example: IPO1.CICS.CICSTS41.TRN:CICSSTC.CEMT. Maximum length: 44 characters.

QUEUE_LOCAL

This field specifies whether local queuing on the local system is to be performed. Field value: Yes or No.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE. You can use the UNIVERSAL modifier to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_CLASS

This field contains the resource class of the profile that protects the resource. The resource class can be a member class or a grouping class. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 8 characters.

RACF_PROFILE

This field contains the name of the profile that protects the resource. The profile can be a member class profile or a grouping class profile. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 13 characters.

RACF_UACC

This field contains the effective universal access authority (UACC) to the program. The UACC is determined from all grouping and non-grouping resource profiles that describe the program. Field values: NONE, READ, EXECUTE, UPDATE, CONTROL, or ALTER.

RCVY_ACTION

This field specifies the action to be taken during two-phase commit processing when a CICS region fails, or loses connectivity with its coordinator, after the unit of work (UOW) has entered the in-doubt period. If the value is Yes, all changes made to recoverable resources are backed out, and the resources are returned to the state prior to the start of the UOW. If the value is No, all changes made to recoverable resources are committed, and the UOW is marked as completed. Field value: Yes or No.

RCVY_DTIME

This field specifies the amount of time (mmss) that CICS waits before it determines a deadlock time-out has occurred and purges the task.

RCVY_DUMP

This field specifies whether a call is made to the dump domain to produce a transaction dump if the transaction terminates abnormally. Field value: Yes or No.

RCVY_RESTART

This field specifies whether a transaction restart facility is used to restart tasks that terminated abnormally and were subsequently backed out by the dynamic transaction backout facility. Field values: Yes or No.

RCVY_RUNAWAY

This field specifies the maximum amount of time (in milliseconds) that a task running under this transaction can have control of the processor before it is assumed to be in a runaway condition (logical loop). When this interval expires, CICS can abnormally terminate the task.

- **0** - There is no limit and no runaway task detection is required for the transaction
- **milliseconds** - The runaway time limit is 500 to 2700000 milliseconds.

RCVY_RUNAWAY_SYSTEM

This field specifies ICVR system initialization parameter value and contains the amount of time, in milliseconds, that any task running under this transaction can have control of the processor before it is assumed to be in a runaway condition (logical loop). When the interval expires, CICS can abnormally terminate the task.

RCVY_SPURGE

This field specifies whether the transaction is initially "system purgeable" or not. Field value: Yes or No.

RCVY_TPURGE

This field specifies, for non-VTAM terminals only, whether the transaction can be purged because of a terminal error. Field value: Yes or No.

RCVY_WAIT

This field specifies whether an in-doubt unit of work (UOW) is to wait, pending recovery from a failure that occurs after the UOW has entered the in-doubt state. Field value: Yes or No.

RCVY_WAITTIME

This field specifies how long a transaction waits for an in-doubt unit of work before taking the action specified in the ACTION attribute. RCVY_WAITTIME is used only if RCVY_WAIT=Yes.

- **00,00,00** - The transaction waits indefinitely.
- **dd,hh,mm** - The time, in days, hours, and minutes, for which the transaction is to wait. The maximum value is 93,23,59.

RESOURCE

This field specifies the resource name that is used to secure the CICS transaction. Maximum length: 246 characters. Default length: 13 characters.

RESOURCE_LOCATION

This field indicates the environment where the resource is relevant. This field is the concatenation of several fixed strings, fields and lookups, such as: *system*.CICS.*jobname*.TRN. An example value is IPO1.CICS.CICSTS41.TRN. Maximum length: 30 characters.

RMT_DYNAMIC

This field specifies whether the transaction can be dynamically routed to a remote CICS region. Field value: Yes or No.

RMT_NAME

This field specifies the name by which the transaction is known in the remote CICS region. Maximum length: 8 characters.

RMT_ROUTABLE

This field specifies whether the transaction is the subject of an eligible EXEC CICS START command, it will be routed using the enhanced routing method. Field value: Yes or No.

RMT_SYSTEM

This field specifies the name of a remote CICS region to which the transaction attach request is sent. Maximum length: 8 characters.

RMT_TRANPROF

This field specifies the name of the profile for the session that carries intersystem flows during ISC transaction routing. Maximum length: 8 characters.

SEC_CMD

This field specifies whether command security checking is to be used for resources accessed by this transaction. If the value is Yes, an external security manager, such as RACF, is used. Field value: Yes or No.

SEC_RES

This field specifies whether resource security checking is to be used for resources accessed by this transaction. If the value is Yes, an external security manager, such as RACF, is used. Field value: Yes or No.

STEPNAME

This field contains the step name associated with the CICS region. Maximum length: 8 characters.

SYSIDNT

This field specifies a 1-to 4-character name to identify your local CICS region. Maximum length: 4 characters.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

TRACE

This field specifies whether the activity of this transaction is to be traced. Field value: Yes or No.

TRACE_CONFDATA

This field specifies whether CICS is to suppress user data from CICS trace entries. Field value: Yes or No.

TRAN_ALIAS

This field specifies an alias transaction name for this transaction. Maximum length: 4 characters.

TRAN_CLASS

This field specifies the name of the transaction class that the transaction belongs to. A transaction class imposes scheduling constraints on transaction execution. Maximum length: 8 characters.

TRAN_ISOLATION

This field specifies whether CICS isolates the transaction's user-key task-lifetime storage in order to provide transaction-to-transaction protection. Field value: Yes or No.

TRAN_PROFILE

This field specifies the name of the profile definition that specifies the processing options used in conjunction with the terminal that initiated the transaction. Maximum length: 8 characters.

TRAN_SHUTDOWN

This field specifies whether the transaction is able to run during CICS shutdown. Field value: Yes or No.

TRAN_TASKREQ

This field specifies whether a transaction is to be initiated by pressing a PF key, by using a light pen, or by using a card. The possible values are as follows:

- **PA1, PA2, or PA3** for PA keys.
- **PF1 through PF24** for PF keys.
- **OPID** for the operator identification card reader.
- **LPA** for a light-pen-detectable field on a 3270 device.
- **MSRE** for the 10/63 character magnetic slot reader.

TRAN_TPNAME

This field specifies the name of the transaction that might be used by an APPC partner if the 4-character length limitation of the TRANSACTION attribute is too restrictive. Maximum length: 64 characters.

TRAN_XTRANID

This field specifies another name to be used to initiate transactions instead of the transaction name. The name might be up to 8 hexadecimal digits in length.

TRANSACTION

This field specifies the name of the CICS transaction. Maximum length: 4 characters.

TWASIZE

This field specifies the size (in bytes) of the transaction work area to be acquired for this transaction. The possible values are: 0 to 32767.

VTAM_APPLID

This field specifies the specific VTAM application identifier (APPLID) for the CICS region. Maximum length: 8 characters.

CLASS: RACF Class Descriptor Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

This section documents the fields for the CLASS NEWLIST. Unless otherwise stated, all fields can be used for SELECT or EXCLUDE processing as well as in the output commands (LIST, SORTLIST, DISPLAY, and SUMMARY).

IBM ships the definition of many classes in an assembled module called ICHRRCDX, the IBM-part of the Class Descriptor Table (CDT). The classes included in the CDT are known as *standard classes*. An installation can add classes to RACF in an assembled module called ICHRRCDE. The classes in this module are known as *user-defined classes*, although many of them are mandated by third-party products. Together, the ICHRRCDX and ICHRRCDE modules are called the static CDT.

Classes can also be defined dynamically, using profiles in the class CDT in z/OS release 1.6 and later. Through the CDTINFO segment, each CDT profile describes a dynamic class. A CDT profile cannot redefine a class defined in the static CDT. In order to avoid potential name conflicts with classes in the ICHRRDCX module, use at least one numeric or national character (#, @, $) in the names of your classes. A warning is issued if you create a profile definition without one of these characters, but the profile is still created. However, if a name conflict occurs, the definition in the ICHRRCDX module takes precedence over any user-defined definition.

The CLASS NEWLIST combines the Class Descriptor Table (CDT) and class-specific SETROPTS options as RACF is using them, which is represented by the incore bits as they are captured in the CKFREEZE snapshot for each system. This class also has additional fields with profile counts that are read from the RACF database if any of those fields are requested. The CLASS NEWLIST provides an alternative to the built-in SHOW CLASSES report. This NEWLIST generates one entry per class in the CDT per system. SYSTEM CLASS is not a guaranteed unique key because a single system can have the same class in both the static CDT and in CDT profiles, which is an acceptable configuration during a short migration period. A single system can also have duplicate profiles within the static CDT, which is considered an error.

The DATASET class is not part of the CDT. For completeness it is shown using a simulated CDT record. Class activity options for the DATASET class are included in this simulated CDT record. They can also be displayed with NEWLIST TYPE=SYSTEM.

Field descriptions

The CLASS NEWLIST provides the following fields for reporting.

ACTIVE

RACF protection for this class is active as a result of a SETROPTS CLASSACT command. This field supports overtype.

AUDIT

Command auditing for this class is active as a result of a SETROPTS AUDIT command. This field supports overtype.

AUDITCONCERN,CONCERN

This field returns a concatenation of audit concerns for the class. The following table shows the default audit priority when active and when not active and provides a description of the associated audit concern. It is sorted by highest audit priority without a policy statement.

Table 325. Default audit priority values and descriptions for active and inactive

Active	Inactive	Audit concern
35	3	SAF calls not processed (not in router table)
35	2	Generics present but not used
25	15	GENCMD off but GENERIC on
	24	Operators are completely unrestricted, no granularity / not B1 compliant
	23	No protection against hackers masquerading as app to steal pwd / not B1 compliant
	22	No protection against hackers masquerading as TP server to steal info / not B1 compliant
	22	Devices like ESCON directors, FEPs, local terminals unprotected / not B1 compliant
	21	No granularity in securing LLA and system services / not B1 compliant
20	20	*settings* difference between database and storage
	20	Temporary data sets resident after failure are unprotected / not B1 compliant
15	3	UACC greater than READ
15	2	GENCMD on but GENERIC off
15	2	Violations not logged - LOGOPTIONS(NEVER)
15	1	UNIX ID uniqueness not enforced by SHARED.IDS profile
15		UNIX options not active because class not RACLISTed
	12	Spooled output not subject to RACF controls / not B1 compliant
11	2	Profile changes in class are not audited
	10	TSO authorities not controlled through RACF, no audit trail / not B1 compliant
	10	JES local node cannot be determined by RACF, spool offload unusable / not B1 compliant
10	1	OPERATIONS honored
10	1	Default RACMAP filter maps to unrestricted user ID
6	1	Default RACMAP filter maps to unprotected user ID
5	1	UACC based on connect group
5	1	UACC greater than NONE
5	1	SETROPTS GLOBAL inactive, but profile present
	5	Profile present but class inactive
1	1	UACC greater than NONE (IBM default)
1	1	UACC based on connect group (IBM default)
1	1	OPERATIONS honored (IBM default)
1	1	Installation defined
	0	Message receivable not subject to MAC / not B1 compliant
	0	Prints are not labelled / not B1 compliant
	0	Security labels are not used / not B1 compliant
	0	Message exchange not controlled / not B1 compliant

Table 325. Default audit priority values and descriptions for active and inactive (continued)

Active	Inactive	Audit concern
	0	Input devices must have a defined security label / not B1 compliant
0		DASDVOL does not implement MAC / not B1 compliant
0	0	No mandatory logging / not B1 compliant

The priority is 40 higher if the concern is not compliant to the policy that has been selected. A priority of 0 means the concern is not issued unless the policy has explicitly been requested.

The following audit concerns have been defined:

- **DASDVOL does not implement MAC / not B1 compliant**

  The DASDVOL class is active on this system. DASDVOL does not honor security labels, and should as such not be used on a B1 compliant system.
- **Devices like ESCON directors, FEPs, local terminals unprotected / not B1 compliant**

  When the DEVICES class is inactive, there is no control over which users can allocate unit record devices, teleprocessing or communications devices, and graphics devices.
- **GENCMD off but GENERIC on**

  For this class the generic command processing has been turned off, while the class is being used as a generic class. Newly created profiles would turn out to be DISCRETE profiles, even if they contain generic characters. This situation should not occur.
- **GENCMD on but GENERIC off**

  The creation and deletion of generic profiles is possible, but RACF does not use them for access control. This could lead to data that is unprotected against expectations. This situation is intended for use when migrating from discrete profiles to generic profiles.
- **Generics present but not used**

  This discrete class contains generic profiles. These profiles are not used by RACF. These profiles can be deleted after turning on generic command processing for the class, using SETROPTS GENCMD(class).
- **Input devices must have a defined security label / not B1 compliant**

  The TERMINAL class is not active. For B1 compliancy it is necessary for each terminal to have a security label defined, so only appropriate data can be accessed via each terminal. This allows better physical security around highly sensitive data access.
- **Installation defined**

  This class is installation defined. Though not necessarily dangerous, this class warrants extra alertness in comparison to defined IBM classes.
- **JES local node cannot be determined by RACF, spool offload unusable / not B1 compliant**

  The &RACLNDE profile in the RACFVARS class is necessary for spool reload functions.
- **Message exchange not controlled / not B1 compliant**

The SMESSAGE class can be used to control which users or groups can send messages to which users. When the SECLABEL class is active, automatic checking of the security label set by the sender against that of the receiver is done as well.

- **Message receipt not subject to MAC / not B1 compliant**

  The DIRAUTH class can be used to block users from receiving any messages with a `seclabel` higher than the one with which they logged on. This also enables auditing of message receipt.

- **No granularity in securing LLA and system services / not B1 compliant**

  In the FACILITY class the possibility exists to define profiles to control access to Library LookAside managed data sets and multiple system services.

- **No mandatory logging / not B1 compliant**

  An access to a profile in the class is not always logged. The concern applies to the DEVICES, DIRAUTH, JESSPOOL, OPERCMDS, PSFMPL, and SMESSAGE classes. It reflects the SETROPTS LOGOPTIONS(ALWAYS(CLASS)) setting.

- **No protection against hackers masquerading as app to steal pwd / not B1 compliant**

  When the VTAMAPPL class is inactive, there is no control over which users can open the application control block (ACB) indicated by a VTAM application program.

- **No protection against hackers masquerading as TP server to steal info / not B1 compliant**

  When the APPCSERV class is inactive, you cannot ensure that only authorized server programs are allowed to serve a particular TP.

- **`OPERATIONS` honored**

  Granting userids with OPERATIONS access to resources within this class, by default, is dangerous and might expose resources in an unintended fashion. Carefully review the need for this class to allow OPERATIONS.

- **`OPERATIONS` honored (IBM default)**

  Granting userids with OPERATIONS to access to resources within this class, by default, is dangerous and might expose resources in an unintentional fashion. Even though it is the IBM default for this class, a careful review might be appropriate.

- **Operators are completely unrestricted, no granularity / not B1 compliant**

  When the OPERCMDS class is inactive, anyone at a master console or a console with system authority is able to use all operator commands.

- **Default RACMAP filter maps to unrestricted user ID**
  Default RACMAP filter maps to unprotected user ID

  Based on the RACF security guidelines, a default RACMAP filter must be mapped to a RACF user ID that is restricted and protected. The default RACMAP filter applies to any user ID in any registry that does not match a more specific filter. Mapping the default filter to a restricted `userid` prevents granting too much access to web users. Mapping the default filter to a protected `userid` prevents locking users out because of an expired password, and prevents the userid from being revoked by a Denial-of-Service attack using the wrong passwords.

- **Prints are not labelled / not B1 compliant**

  If Print Services Facility/MVS (PSF/MVS) is installed, the PSFMPL class can be used to force labeling of all prints and granting the possibility of overriding this to selected users.

- **Profile changes in class are not audited**

  Changes to profiles in the class (by using the RDEFINE, RALTER, RDELETE, and PERMIT commands) are not always logged. This concern reflects the SETROPTS AUDIT(CLASS) setting.

  Note that profile changes are logged if SPECIAL users execute the commands while the SETROPTS SAUDIT setting is active.

- **Profile present but class inactive**

  The SAF (System Authorization Facility) router returns the default return code from the CDT (most often RC=4, which indicates an indeterminate result) for any SAF check in these classes, and RACROUTE calls do not use profiles in these classes. RACF can use these profiles using the RACHECK interface, leading to conflicts between SAF and direct RACF calls.

- **SAF calls not processed (not in router table)**

  This class is not found in the router table. This means that RACF returns the "not protected" return code. Most applications grant access in this situation. On z/OS V1R6 and higher systems the router table is optional, and this audit concern is no longer generated.

- **Security labels are not used / not B1 compliant**

  The security label system (SECLABEL class) can be used to dramatically increase the granularity of access control throughout your system. It is one of the basics of B1 security.

- **`SETROPTS GLOBAL` inactive, but profile present**

  This suggests that somebody wanted to add entries for this class to the global access table, but did not succeed in doing so.

- *`settings`* **different between database and storage**

  This indicates that the indicated settings in the system's RCVT (the actual in-storage bits being tested by RACF) differ from the settings stored on DASD in the RACF database ICB. This is probably caused by combining a CKFREEZE file and RACF database of different systems or by combining snapshots of different dates or time. Although less likely, it can also be caused by an attacker changing the in-storage settings. The value *settings* can be one or more of the following: STATS, AUDIT, ACTIVE GENERIC, GENCMD, GLOBAL, RACLIST, GENLIST, LOGALWAYS, LOGNEVER, LOGSUCCESS, and LOGFAILURE.

- **Spooled output not subject to RACF controls / not B1 compliant**

  The JESSPOOL class can be used to control all JES2 or JES3 spool files. When activating this class, the default is that only the user who created the spool file has any access to it, but profiles can be created to allow others access.

- **Temporary data sets resident after failure are unprotected / not B1 compliant**

  The TEMPDSN class is inactive. After activating this class, only users with the OPERATIONS attribute have access to temporary data sets left after a system failure, and then only to scratch these data sets. With TEMPDSN inactive these data sets are completely unprotected by RACF and most applications grant access in this case.

- **TSO authorities not controlled through RACF, no audit trail / not B1 compliant**

  Any one of the classes ACCTNUM, TSOPROC, or TSOAUTH is not active. This means that for access to these resources, TSO/E uses the information as stored in SYS1.UADS. RACF control and auditing are not possible for account numbers, logon procedures, and most TSO authorizations. In this situation,

the CONSOLE, PARMLIB and TESTAUTH functions are not available. Auditing of the TSOAUTH authorizations, except for the PARMLIB command is always suppressed by TSO/E.

- **UACC based on connect group**

  Whenever you create a profile in this class and do not specify an explicit UACC the UACC is copied from the current connect group. This means it depends on which userid and group name a user specified at logon time. Hence it is rather easy to issue a UACC too that is too high by mistake.

- **UACC based on connect group (IBM default)**

  Whenever you create a profile in this class and do not specify an explicit UACC the UACC is copied from the current connect group. This means it depends on which userid and group name a user specified at logon time. Hence it is rather easy to issue a UACC too that is too high by mistake.

- **UACC greater than NONE**

  Setting the default access level higher than NONE is not advised. Although this setting might be appropriate in some circumstances, it is a good idea to review the setting to ensure that resources are not accidentally exposed to unnecessary read access.

- **UACC greater than NONE (IBM default)**

  Setting the default access level higher than NONE is not advised. Although this setting is the IBM default, it is a good idea to review the setting to ensure that no sensitive data is accidentally exposed.

- **UACC greater than READ**

  It is unusual for a protected resource to have default access above READ, although NONE is preferable. This might be appropriate, but bears a review to ensure that resources are not accidentally exposed to update or greater access.

- **UNIX ID uniqueness not enforced by SHARED.IDS profile**

  To control the use of shared IDs, a resource profile called SHARED.IDS can be defined in the UNIXPRIV class. When this profile is absent the use of shared user and group IDs is not protected.

- **UNIX options not active because class not RACLISTed**

  The UNIXPRIV class has to be RACLISTed for the profiles in this class to be used.

- **Violations not logged - LOGOPTIONS(NEVER)**

  This is undesirable since violations would not be journaled to SMF. Journaling violations and follow-up tracking is critical to securing the resources within an installation.

AUDITPRIORITY

This field returns the audit priority for the concern. See field AUDITCONCERN for a table with the concerns and their priorities. The actual audit priority can be higher or lower because of differences between classes and e.g. a SIMULATE POLICY C2 statement.

CASE_ASIS

This flag field indicates whether profile names for this class are kept as is or are converted to upper case. This field has a flag format where "Yes" means that the case is preserved, and "No" means that names are converted to uppercase. For very old RACF systems, the value is blank. This also means that names are converted to uppercase.

CLASS, C

Class name of current entry.

CLASSNO

This is an alias of ORG.

CLAUTH

The class authorization field CLAUTH is a repeating field that includes the eight-character RACF user IDs that can administer the specified class. These user IDs include those that have a class with the same POSIT number as the specified class in their CLAUTH list, although they do not specifically have the class on the CLAUTH parameter. The CLAUTH authority can be limited by the SETROPST GENERICOWNER specification. However, for classes that have an associated grouping class that is RACLISTed, a CLAUTH user can subsume any generic general resource profile with a discrete profile that does not exist yet as a member profile or a group profile member–independently of the GENERICOWNER setting.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can come from the ALLOC COMPLEX parameter or default to a system name.

DATASPC

This flag indicates whether RACLISTed profiles for this class have been stored in a dataspace.

DESCRIPTION

This 64 character field returns a short explanation of the purpose of the class.

DFLTRC

This field contains the default return code for this class. This code is returned when no matching profile can be found at a RACHECK. The result codes and their meaning are documented in the following table.

Table 326. Result code values and descriptions

DFLTRC value	Meaning
0	Allow access
4	Indeterminate: depends on resource manager
8	Fail access

EQUALMAC

This flag field indicates whether equal mandatory access checking is required for resources in this class. This means that in order to be granted access to a resource, the SECLABEL of the user and the resource must be equivalent (have the same security level and categories). This setting is used only when the SECLABEL class is active.

GEN

This string is set to '**Discrete**' if generic profiles in this class are not checked, and is empty otherwise.

GENCMD

Generic profile command processing for this class is active (due to a SETROPTS GENCMD or a SETROPTS GENERIC command). This field supports overtype.

GENERIC

Generic profile checking for this class is active (due to a SETROPTS GENERIC command). This implies that generic command processing for this class is active. This field supports overtype.

GENERIC_ALLOWED

Flag field that indicates whether SETROPTS GENERIC and SETROPTS GENCMD are authorized for the class. The value corresponds to the CDTGEN field in the `RACF NEWLIST (NEWLIST TYPE=RACF)` , see "CDTGEN" on page 1137.

GENLIST

This flag indicates that this class has been GENLISTed, which means that generic profiles for this class are retained in storage that is shared between address spaces based on a SETROPTS GENLIST command. If this flag is set, the RACLIST flag cannot be set. This field supports overtype.

GENLIST_ALLOWED

Flag field that indicates whether this class can be GENLISTed. That is, generic profiles for this class can be retained in storage that is shared between address spaces (by using the SETROPTS GENLIST command).

GLB

String indicating global access checking activity. Note that for older RACF versions, global access checking and SETROPTS RACLIST cannot be combined; if this appears to be the case, this string is set to `n/a`. Otherwise, it is set to `Glob` if global access checking is active, and blank if global access checking is inactive.

GLOBAL

Flag indicating Global Access Checking activity. Undefined if no Global Access checking is allowed, set if Global Access checking is active, and not set if Global Access checking is inactive. This field supports overtype.

ID

Generic class identifier. This is a number in the range 0 to 255 that is associated with the class name in the Class Descriptor Table and also stored in the CLASTYPE field of general resource profiles in the RACF database. Numbers 1 through 127 are reserved for use by IBM; numbers 128 through 255 are installation-dependent.

INRFR

This flag indicates whether the current class is included in the SAF (System Authorization Facility) router table (see NEWLIST TYPE=ROUTER). On z/OS V1R6 and higher systems the router table is optional. On those systems a 'No' is interpreted as if an entry with ACTION=RACF were present. On older systems any 'No' indicates a mismatch and RACROUTE requests for this class return an 'indeterminate' result (RC=4).

INSTALLATION_DEFINED

This flag indicates whether the class is user-installed (for example, not IBM-defined).

LOGOPT

Auditing options for this class, due to a SETROPTS LOGOPTIONS command. The LOGOPT values and the SETROPTS LOGOPTIONS auditing level are documented in the following table.

LOGOPT value	SETROPTS LOGOPTIONS auditing level
Always	ALWAYS
Failure	FAILURES
Never	NEVER
Profile	(determined by profile)
Success	SUCCESSES

This field supports overtype.

MAXLEN

This field contains the maximum length of profile names in this class. This is a number in the range 1 to 246. See also MAXLEN_ENTITY.

MAXLEN_ENTITY

This field specifies the backward compatible maximum profile name length to be used with the ENTITY keyword form of the RACROUTE macro. This macro form does not pass the return buffer length; if the maximum profile name length increases, existing applications might break if the entire profile names were returned. IBM recommends that the ENTITYX keyword form of RACROUTE is used, to which this limit does not apply. This is a number in the range 1 to 246; the default is 8. See also MAXLEN (the true maximum profile name length).

NOPROF

Flag indicating whether profile definition is forbidden in this class. If set, users cannot use the RDEFINE command to define profiles.

NUMDISC

Number of discrete profiles in this class.

NUMGEN

Number of generic profiles in this class.

NUMPROF

Number of profiles in this class (NUMDISC plus NUMGEN).

OPER

This flag field indicates whether OPERATIONS authority is honored for this class.

OPEROPER

This is a string representation of the OPER field. It contains the text '**OPER**' if OPERATIONS authority is honored for this class, and is empty otherwise.

ORG, ORDER, CLASSNO

The original order (entry number) of this class in the class descriptor table. The first entry in the table has ORDER=1.

POSIT

This field contains the options set id, a number in the range 0 to 1023 identifying a set of SETROPTS options that govern the activity of this class and all other classes having the same POSIT value. Whenever a SETROPTS command is issued for any class with a specific POSIT value, it applies to all classes with that same POSIT.

POSIT values in the range 0-18, 57-127, and 528-1023 are reserved for use by IBM; numbers 19-56 and 128-527 are installation-dependent.

PROTECT

This is a string summarizing the protection options for this class and is based on the ACTIVE and AUDIT flags. The PROTECT values and the related values of the ACTIVE and AUDIT flags are documented in the following table.

Table 327. PROTECT value descriptions and associated flags

PROTECT value	ACTIVE flag	AUDIT flag
Inactive	NO	-
Noaudit	YES	NO
(blank)	YES	YES

QUAL

This field contains the number of qualifiers at the start of the profile name that cannot be generic. This is a number in the range 0 to 123; the default is 0. During access verification, RACF ignores all profiles that have generic characters in the specified number of qualifiers. This also controls which profiles are loaded (and kept) in storage.

RACLIST

This flag indicates that this class has been RACLISTed, which means that both generic and discrete profiles for this class are loaded into storage that is shared between address spaces (due to a SETROPTS RACLIST(class) command). If this flag is set, the GENLIST flag cannot be set. This field supports overtype.

RACLIST_ALLOWED

Flag field that indicates that this class can be RACLISTed by issuing the SETROPTS RACLIST command. When a class is RACLISTed, both discrete and generic profiles are loaded into storage that is shared between address spaces. Generally, this flag is turned off if only an application is supposed to request a RACLIST. See also RACLREQ and RACLIST_GBL_ONLY.

RACLIST_GBL_ONLY

Flag field that indicates that this class is currently RACLISTed to a dataspace only because an application issued a `RACROUTE REQUEST=LIST` with `GLOBAL=YES`. Applications like CICS and IMS use this function to allow efficient use of `RACROUTE REQUEST=FASTAUTH` for checking user authorizations. For SETROPTS RACLISTed resource classes, RACF issues a warning message if a `SETROPTS RACLIST REFRESH` is required for the resource class to make the changes effective. RACF does not issue such a warning message for `GLOBAL ONLY RACLISTed` resource classes. Although RACF does not issue the warning, you still need to issue the `REFRESH` to make changes to such a class effective.

When applicable, this flag is set for grouping and member classes.

RACLREQ

Flag field That indicates that this class must be RACLISTed. When a class is RACLISTed, both generic and discrete profiles are loaded into storage that is shared between address spaces.

RVRSMAC

This flag field indicates whether reverse mandatory access checking is required for resources in this class. This means that the SECLABEL of the resource must dominate the SECLABEL of the user. This setting is used only when the SECLABEL class is active. See also EQUALMAC.

SAME_POS

This repeated field contains the classes that have the same POSIT value as this class. Whenever a SETROPTS command is issued for any class with a specific POSIT value, it applies to all classes with that value. This field lists all classes in the CDT, not only the active ones.

SECLABEL

This flag field indicates whether security labels are required for resources in this class. When the SECLABEL class is active and a security label exists for a resource, the security label for the resource is used during authorization checking, even when security labels are not required.

SIGNAL

This flag field indicates whether an ENF signal must be sent when the class is being RACLISTed, NORACLISTed, or RACLIST REFRESHed.

STATS

Flag indicating whether statistics are collected for this class (due to a SETROPTS STATISTICS command). This field supports overtype.

SYN1ALP

Flag field that indicates if the first character of a profile in this class can be alphabetical. Combine this flag with the SYN1NAT, SYN1NUM and SYN1SPE flags to determine all legal first characters.

Note: These flags do not match the input parameters used to build the Class Descriptor Table. The following table documents the input parameter values and their correspondence to the SYN1ALP, SYN1NAT, SYN1NUM and SYN1SPE flags and the combination field SYN1RAW

Table 328. Input parameters values and character flag settings

Input value	SYN1ALP	SYN1NAT	SYN1NUM	SYN1SPE	SYN1RAW
ALPHA	Yes	Yes	No	No	C0
ALPHANUM	Yes	Yes	Yes	No	E0
ANY	Yes	Yes	Yes	Yes	F0
NONATABC	Yes	No	No	No	80
NONATNUM	Yes	No	Yes	No	A0
NUMERIC	No	No	Yes	No	20

SYN1NAT

Flag field that indicates if the first character of a profile can be a national character (#, @ and $). Combine this flag with the SYN1ALP, SYN1NUM and SYN1SPE flags to determine all legal first characters. See also the table at the SYN1ALP field.

SYN1NUM

Flag field that indicates if the first character of a profile in this class can be a numeric character. Combine this flag with the SYN1ALP, SYN1NAT and SYN1SPE flags to determine all legal first characters. See also the table at the SYN1ALP field.

SYN1RAW

This field contains the raw value of the syntax rules for first character of profile in this class. It is a combination of the corresponding flags SYN1ALP, SYN1NAT, SYN1NUM and SYN1SPE. To interpret the value of this field, see also the table at the SYN1ALP keyword.

SYN1SPE

Flag field that indicates if the first character of a profile in this class can be a special character–any character other than alphabetical, numerical, national, blank, comma, parenthesis or semicolon. Combine this flag with the SYN1ALP, SYN1NAT and SYN1NUM flags to determine all legal first characters. See also the table at the SYN1ALP field.

SYNRALP

Flag field that indicates if all characters other than the first character of a profile in this class can be alphabetical. Combine this flag with the SYNRNAT, SYNRNUM and SYNRSPE flags to determine all legal characters.

Note: These flags do not match the input parameters used to build the Class Descriptor Table. The following table documents the input parameter values and their correspondence to the SYNRALP, SYNRNAT, SYNRNUM and SYNRSPE flags and the combination field SYNRRAW.

Table 329. Input parameter values and character flag settings

Input value	SYNRALP	SYNRNAT	SYNRNUM	SYNRSPE	SYNRRAW
ALPHA	Yes	Yes	No	No	C0
ALPHANUM	Yes	Yes	Yes	No	E0
ANY	Yes	Yes	Yes	Yes	F0
NONATABC	Yes	No	No	No	80
NONATNUM	Yes	No	Yes	No	A0
NUMERIC	No	No	Yes	No	20

SYNRNAT

Flag field that indicates if all characters other than the first character of a profile in this class can be a national character (#, @ or $). Combine this flag with the SYNRALP, SYNRNUM and SYNRSPE flags to determine all legal characters. See also the table at the SYNRALP field.

SYNRNUM

Flag field that indicates if all characters other than the first character of a profile in this class can be a numeric character. This flag must be combined with the SYNRALP, SYNRNAT and SYNRSPE flags to determine all legal characters. See also the table at the SYNRALP field.

SYNRRAW

Contains the raw value of the syntax rules for the remainder characters of a profile name in this class. It is a combination of the corresponding flags SYNRALP, SYNRNAT, SYNRNUM and SYNRSPE. To interpret the value of this field, see the table at the SYNRALP field.

SYNRSPE

Flag field that indicates whether all characters other than the first character of a profile in this class can be a special character–any character other than alphabetical, numerical, national, blank, comma, parenthesis, or semicolon. Combine this flag with the SYNRALP, SYNRNAT and SYNRNUM flags to determine all legal first characters. See also the table at the SYNRALP field.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters to cater to VM systems.

UACC

This field contains a character string with the default Universal ACCess for this class. This default UACC is used to set the profile UACC during addition of a profile in this class if no UACC is specified on the command. Possible UACC values are documented in the following table. The special value ACEE indicates that the value UACC is taken from the default UACC in the user's ACEE (specified by UACC on the ADDUSER, ALTUSER or CONNECT command.) Table 330 lists the possible UACC field values in descending sort order. Because this is a string field, the statement SELECT UACC>=UPDATE can return undesired results. Use SELECT UACC=(UPDATE,CONTROL,ALTER) instead.

Table 330. Possible UACC values

UACC value
ACEE
ALTER
CONTROL
NONE
READ
UPDATE

WHERE

This field indicates profile residency. The possible WHERE values and their meaning are documented in the following table.

Table 331. WHERE values and descriptions

WHERE value	Meaning
Genlist	Profiles have been GENLISTed as a result of a SETROPTS GENLIST command. That is, generic profiles are retained in storage shared between address spaces, but discrete profiles are not resident.

Table 331. WHERE values and descriptions (continued)

WHERE value	Meaning
NoGenl	SETROPTS GENLIST is not allowed for this class; SETROPTS RACLIST is, but has not been specified.
NoList	SETROPTS RACLIST and SETROPTS GENLIST are not allowed for this class, usually because applications issue RACLIST themselves.
NoRacl	SETROPTS RACLIST is not allowed for this class; SETROPTS GENLIST is, but has not been specified.
Nowhere	Profiles not allowed in this class.
RaclGbO	The profiles are resident only because they have been RACLISTed by an application via a RACROUTE macro with GLOBAL=YES specified.
Raclist	Profiles have been RACLISTed (due to a SETROPTS RACLIST command), for example reside in a data space or in (E)CSA.
RaclReq	Profiles must reside in-storage if class is active.
(blank)	Class has not been RACLISTed or GENLISTed, but it would be allowed.

XCLASS

Contains the name of the related class. This field only returns a value for grouping or member classes.

XGROUP

For member classes, this field contains the name of the related grouping class. For non-member classes this field is blank. See also XMEMBER.

XMEMBER

For grouping classes, this field contains the name of the related member class. For non-grouping classes this field is blank. See also XGROUP.

CONCERN_TEXT: Concern translation properties

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The CONCERN_TEXT NEWLIST (NEWLIST TYPE=CONCERN_TEXT) enumerates text segments used in audit concern text and is useful to translate audit concern text. It is only supported if zSecure Audit is installed and active.

The default title for this report is: AUDIT CONCERN TEXT DEFINITIONS.

Field descriptions

You can use the following CONCERN_TEXT fields to translate the audit concerns.

CONCERN

Final translated text of the audit concern. Variables can occur in a different place then in the English string.

CONCERN_ID

Unique identification of the concern.

CONCERN_ORIG

The original (English) text for the audit concern. Variables are preceded with a number symbol (#) and end with a period, for example, #1..

NEWLIST_TYPE

The TYPE passed on the NEWLIST statement, optionally suffixed with .DISPLAY if the NEWLIST contains a DISPLAY or DSUMMARY statement, as opposed to only a subset LIST, SORTLIST, or SUMMARY statement.

The key for records of this type is CONCERN_ID.

NEWLIST_TAG

An internal number for the NEWLIST type. This value can change without warning and should not be used as a programming interface.

CONSOLE: System Consoles

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The CONSOLE NEWLIST (NEWLIST TYPE=CONSOLE) describes the system consoles defined on the target systems. Each entry in this NEWLIST represents one console. EMCS consoles are only present when the CKFREEZE data has been collected from an APF-authorized run of zSecure Collect.

Field descriptions

The CONSOLE NEWLIST provides the following fields for reporting.

ACTIVE

Flag field that indicates whether the console is active or not. For a subsystem console, it is shown as Yes when the console is dedicated to a subsystem, and No if it is in allocatable status.

ALTERNATE

This field describes the name of the alternate console, or the console group that will serve as an alternate. It contains the alternate console group (ALTGRP), or the alternate console's name (possible until z/OS 1.4), or has the format **xxx** or **xxx,xxx** describing the alternate console's device number(s). This field is 9 characters in length.

This field is not present in z/OS V1R8 and higher systems.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas. The following audit concerns are currently defined:

Table 332. Audit concern priority descriptions

Active	Inactive	Meaning

Table 332. Audit concern priority descriptions (continued)

25	65	**System authority and no logon required, any terminal may connect (SMCS LU not predefined)** This concern indicates that an explicit LOGON must be specified in CONSOL*xx* because the default for non-predefined SMCS consoles is to use LOGON=REQUIRED. This condition is unsafe condition because any terminal can issue a LOGON APPLID for the SMCS VTAM application, and operator commands can be issued without the user being authenticated. It then depends on the SAF (System Authorization Facility) class OPERCMDS to determine exactly which commands are permitted or disallowed. This is a violation of B1 policy.
20	60	**System authority and no logon required** The console's authority includes system commands, but the system does not require logons for any console. You should check that the console, the alternate console, and all subsequent alternate consoles, reside in a secure area. This must condition can only be created by an explicit LOGON specification in CONSOLxx, since the default for non-predefined SMCS consoles is to use LOGON=REQUIRED. It depends on the SAF class OPERCMDS exactly which commands are allowed or disallowed. This is a violation of B1 policy.
15	55	**Any terminal may connect and is logged on automatically without authentication (SMCS LU not predefined)** This SMCS console is available to any terminal (LU) and automatically logs on with a RACF userid equal to the console name without requiring authentication. The OPERCMDS class restricts what commands can be issued.
5	5	**No logon required, any terminal may connect and obtain information (SMCS LU not predefined)** This SMCS console is available to any terminal (LU) and does not require a LOGON. The console does not have the authority to issue commands that require SYSTEM or MASTER authority, but it allows commands that display information. This can help a hacker in obtaining inside information like lists of userids he can then to guess passwords for.
2	2	**Autologon specified but RACF user undefined** The console will not function. It is not a security risk but a housekeeping issue, unless the console has a critical role for some reason.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 333. CONSOLE NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

AUTH

This field describes the AUTH parameter of the console, which specifies the MVS command groups to be executed. This is a string that can contain one or more of the values SYS, IO, CONS, and INFO; if all values are set, the string has the value ALL. For a master console, this string has the value MASTER.

Table 334. AUTH values and descriptions

AUTH value	Meaning
ALL	All command types
CONS	Console commands
INFO	Information commands
IO	Input/output commands
MASTER	Master console
SYS	System commands

Note: This field is implemented as a text string with assigned positions for the possible values. So if a console has only INFO authority the value displayed will be "_____INFO", while a console with both CONS as well as INFO authority will be displayed as "_____CONS INFO" (underscores are used to denote blanks). When a console has all four possible authorizations the string "ALL_____" is used instead of the list of four authorizations. When searching for the consoles that have a particular authority, you should use a list of values. The first two are "ALL" and "MASTER". The other one could use the scan operator ":" or the substring function. Using these three values, you will find all consoles that have the required authorization. For example, to find all consoles with an authorization including "IO", you could use SELECT AUTH=(:IO,ALL,MASTER).

AUTO

Flag field that indicates whether this console is to receive messages that were automated (and possibly suppressed) by the Message Processing Facility (MPF). It is only defined for EMCS consoles. To see which messages are automated, see NEWLIST TYPE=MSG.

CMDSYS

The system that will receive commands typed on the console. It can be "*" to indicate the system where the console is defined. This field length is 8 characters.

CNID

This is the 4 byte console id. It is displayed in hexadecimal by default. It is the id used by programs to route commands responses or messages.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

CONSOLE_NO

This field describes the console number. For EMCS consoles, this field is empty, unless they have a migration id defined.

DEVICE_NO, DEVNUM

This field describes the console's device number. It is not present for a subsystem or EMCS console.

DOM

This fields shows whether the console receives Delete Operator Messages (DOM) and from where. It can be ALL (all systems in sysplex), NORMAL (this system), or NONE (no system). This field can be displayed with formats DOM and $DOM.

HC

Flag field that indicates whether this console is to receive hardcopy-only messages. It is only defined for EMCS consoles.

INTIDS

This flag field indicates whether the console should display internal messages (sent to console 0). It is available since z/OS V1R8.

JOBID

This field can contain the JES job id of the job that has the console allocated. It is only defined for EMCS consoles. This field is max 8 characters.

KEY

The KEY assigned by the OPERPARM data to an EMCS console. This key can be set by the creator of an EMCS console or inherited from the OPERPARM specification in the security product. This is just an identifier that a site can use to easily display a set of consoles. It is only defined for EMCS consoles. This field is max 8 characters.

LEVEL

This field describes the message level for the console. It can only be used for output, not for SELECT/EXCLUDE processing. This field contains the console message level in 14 characters. The first 12 characters can be ALL or a combination of the letters R I CE E IN. The last two characters are NB or blank. The length cannot be changed. The field is not present for subsystem consoles. The meaning of the characters is:

Table 335. LEVEL field - character values and descriptions

Character	Meaning
NB	No broadcast messages
ALL	Same as R I CE E IN
R	Messages requiring an operator reply
I	Immediate action messages
CE	Critical Eventual action messages
E	Eventual action messages
IN	Informational messages

LOGON

This field describes whether a logon is required for a console. It can have the values OPTIONAL, REQUIRED, and AUTO.

Note: On pre-z/OS 1.1 systems, this field is the same for all consoles in the system.

LUNAME

For an SMCS console, the VTAM Logical Unit name. For an EMCS console, the terminal name. This field is max 8 characters.

MIGID

Migration id of an EMCS console. This is a small console number that can be used by applications that do not support 4 byte CNIDs yet.

MONITOR

This field shows the events that must be monitored on the consoles, like JOBNAMES, SESSION, and STATUS. It can be displayed with output formats MONITOR and $MONITOR.

NAME

This field describes the console name.

PFKTAB

This field describes the PF-key table used; these tables are defined in SYS1.PARMLIB member PFKTABxx.

RACF_PROFILE

This field shows the profile name for the profile protecting the console. It is blank if there is no such profile or the CONSOLE class is inactive.

ROUTECODE, ROUTCODE

This field describes the routing codes for the console. It can only be used for output, not for SELECT/EXCLUDE processing. The routing code is displayed as a list of routing code ranges, separated by commas.

SUBSYSTEM

This field describes the subsystem to which the console is dedicated, if the TYPE field is set to SUBSYSTEM, and the console is in use by a subsystem. For an EMCS console, this contains the jobname that has the console allocated. In other cases, this field is blank. Maximum length: 8 characters.

As this field mostly contains a jobname the default column header for this field is "Jobname".

SWITCHTO

This field shows the name of a console to which this console has been switched. Normally, it is empty. The field length is 8 characters.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. This field length is 8 characters for compatibility with other NEWLIST types.

TYPE

This field describes the type of the console. It can be:

Table 336. Console TYPE values and descriptions

Character	Meaning
EMCS	An extended (programmatic) console. This value can be a subsystem console (TSO/E, SDSF), syslog, or system console.

Table 336. Console TYPE values and descriptions (continued)

Character	Meaning
Master	The master console (this is an MCS console with master authority).
MCS	A traditional console (MCS means Multiple Console Support).
SMCS	A VTAM console accessed through a VTAM LOGON to a site-specific SMCS application id. SMCS means SNA Multiple Console Support.
SubSystem	A subsystem console. This is a console is allocatable to or allocated by a subsystem like Netview.
Syslog	The SYSLOG EMCS console.
DIDOCS	The DIDOCS EMCS console (DIDOCS means Device Independent Display Of Operator Console Support). This was introduced in z/OS 1.5.

UD

This flag field indicates whether the console displays undirected messages (messages that do not go to a specific console). At least one console in the system should receive these messages.

Note: This field is missing for z/OS 1.5 and higher systems.

UNKNIDS

This flag field indicates whether the console should display messages to unknown console ids. It is available since z/OS V1R8.

USERID

This field provides the `userid` of the user logged on to the console. This field might be blank if no user is logged on to the console–if the LOGON field contains OPTIONAL for example,

CSM: Common Storage

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The NEWLIST TYPE=CSM describes the Common Storage Map. This map shows the memory regions that together form the common (shared) part of virtual storage.

This NEWLIST describes the common storage in detail. Another NEWLIST type, NEWLIST TYPE=VSM, describes the layout of all storage areas, but does not include detailed information on individual common storage areas.

Each entry in this NEWLIST represents a single memory block in common storage, and can be uniquely identified by the fields SYSTEM START.

Field descriptions

The `CSM NEWLIST` provides the following fields for reporting.

AUDITCONCERN

This field indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs. The field content might change. The audit concern currently defined is:

Memory region writable by any user
This audit concern means that an attacker can modify the behavior of an application running in the address space of another user. The amount of damage this situation can cause depends on the application. This situation also highlights that the application has not been designed with proper security in mind. The exposure might be relatively simple to exploit and might compromise the entire system integrity. This problem is obvious if the memory area contains code that is run while in supervisor state or key zero. That latter situation is checked and reported in other `NEWLIST` types like SVC routines, PC routines, subsystem routines, and so on.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 337. CSM NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can be taken from the ALLOC COMPLEX parameter or default to a system name.

END

The end address of a storage area. This value is either an 8 character (4 byte) hexadecimal number or two 8 character hexadecimal numbers separated by an underscore for 8 byte addresses (possibly) situated above the 4 GB threshold.

FPROT

This field is a flag indicating the status of storage fetch-protection for this common storage item. This field returns `Yes` or `No` but its default length is 1 so it returns `Y` or `N` by default. Fetch protection of z/Architecture memory is part of the *key-controlled protection facility* of memory.

Key controlled protection supplies the capability of memory protection (at the 4 K page level). Each running program has a 4 bit key associated with it which is stored in the Program Status Word or PSW. Each page of memory also has 4 bit key associated with it. If these keys match or the PSW key is zero, then the program can both read (fetch) data from the memory and write (store) data back to that memory. If the keys do not match, but the request is for fetch, then a further bit related to the page of memory is examined. This bit is the

Fetch-Protection bit. If the Fetch-Protection bit is set ON, then the access is denied. If the Fetch-protection is off, then the access is granted.

For reference, here are some extra notes to clarify the use of fetch protection:

- 31 bit Common storage is organized into subpools. Some of these subpools are Fetch-protected.
- 64 bit Common memory Objects and Shared Memory Objects can be fetch-protected. Fetch-protection is requested at the time the object is created. While key-protection applies at the page level, z/OS does not supply facilities to have differing keys within a single 64 bit memory object.
- If access to storage is denied during either a fetch or store operation, then a protection exception is raised. z/OS normally presents this condition as a System abend 0C4-04.
- If a program is operating in Key 0, then it is given access (both fetch and store) to all memory by the key-controlled memory protection facility. Because the operating system (z/OS) operates predominantly in Key 0, it is unlikely to suffer fetch-protection issues.
- Programs operating in Keys 0 through 7 are considered privileged by z/OS. Programs operating in these keys can use the MODESET macro to alter their own Key or their program state (Supervisor or Problem Program).
- The following privileged keys are assigned to specific z/OS components or major subsystems:
  - Key 1 is used by the Scheduler (JES2 or JES3).
  - Key 5 is used by data management.
  - Key 6 is used by the Communications Server.
  - Key 7 is used by IMS.
- Key 8 storage is the key that most application programs use. Although it might seem that using the same key for storage creates integrity problems for one program accessing the memory of another program, this problem does not normally occur because z/OS protects one address space from accessing the private memory of other address spaces. However, common storage that is in Key 8 can be altered (stored into) by most unprivileged user programs.
- If storage is set to Key 9, then programs in any key can access the storage for both Fetch and Store operations. This facility is used in some major software subsystem such as CICS. The facility is an option in z/Architecture terms, but in practice z/OS always makes the function available.
- Keys 10 through 15 are used for programs which need to run REAL, which means they run without the overhead of page movement. Programs with this requirement are rare.
- Key-controlled protection is one of four types of memory protection available within z/Architecture. In order for a memory access to be granted, all four methods must allow the access of the type requested (fetch or store).

For additional information on hardware memory protection facilities, refer to the *z/Architecture Principles of Operation* manual available in the z/OS documentation library (http://www-03.ibm.com/systems/z/os/zos/bkserv/).

KEY

Contains the storage protection key of a memory area. A key of 8 to 15 characters is cause for concern because any user might be able to change the area.

LENGTH

The length of a storage area. This value is a decimal number of up to 11 digits.

START

The start address of a storage area. This value is either an eight-character (four-byte) hexadecimal number or two eight-character hexadecimal numbers separated by an underscore for eight-byte addresses (possibly) situated above the 4 GB threshold. The difference between START and START64 is that START shows if the address has a high-order fullword in the operating system or not. In addition, the START field does not support address sorting. If sorting is required, use the START64 field.

START64

The start address of a storage area as a 64-bit number. This value is formatted as two eight-character hexadecimal numbers separated by an underscore for eight-byte addresses (possibly) situated above the 4 GB threshold. Use this field to sort by address.

SUBPOOL

This field contains the subpool number of a memory area. It is missing for storage areas located above the bar.

SYSTEM

The name of the system. For MVS systems, this value is equal to the SMF system id. This field has a length of 8 characters for compatibility with other NEWLIST types.

TYPE

A string indicating the virtual storage area type. Table 338 documents the available TYPE values and their descriptions. Areas starting with an E reside above the 16 MB virtual storage threshold. Areas that start with an X reside above the 4 GB virtual storage threshold.

Table 338. Virtual storage area type values and descriptions

TYPE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
ESQA	Extended System Queue Area
SQA	System Queue Area
XCOM	Extended Common Storage Area above the bar
XSHR	Extended Shared Storage Area above the bar (previously called XCSA)

DASDVOL: DASD volumes

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The DASDVOL NEWLIST (NEWLIST TYPE=DASDVOL) describes the DASD volumes available on the target systems. Both shared and non-shared information is taken into account, but has the same restrictions as DASD volumes in Security zSecure. That is, SIMULATE SHARED commands might be required. A CKFREEZE file is required

for each of the systems to which the DASD volumes are connected. Systems to which the DASD volume is connected, but for which no CKFREEZE file is read, are not included in the report.

Each entry in this NEWLIST represents one physical DASD volume. Each entry in this NEWLIST can be uniquely identified by the field ORG.

Because this report is not complex-centric at all, the NEWLIST parameter ESM= is not meaningful for this NEWLIST type.

Field descriptions

The DASD NEWLIST provides the following fields for reporting.

ATTR

Text field that is repeated for each of the target systems to which the DASD volume is attached. The value describes the volume attributes for the current system. This field can contain one or more of the following values: IPL for an IPL-volume, MCAT if the volume contains the master-catalog volume for the system, and PAGE if the volume contains a page data set. This field is part of the structured repeat group described with the SYSTEM field.

AUDITCONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs. The contents might change. The value can contain one or more of the following audit concerns separated by commas.

- **Mounted on one system but shared**

  The DASD volume is mounted on only one system but marked shared. This setting causes unnecessary overhead.
- Mounted on more systems but not shared

  The DASD volume is mounted on several systems but not marked shared. No serialization is done for updating the volume, and if two systems try to update simultaneously, an undefined state can result which can cause loss of data.
- **Inconsistently SMS-managed**

  The DASD volume is mounted on several systems, and SMS-managed on some but not all of these systems. This situation can cause problems with APF-libraries on the volume. Also, when data sets are moved to another volume by SMS, jobs might fail and catalog inconsistencies might appear on systems where the volume is not SMS-managed.
- **Inconsistent SMSplex names**

  The DASD volume is mounted and SMS-managed on several systems. However, the SMSplex (sysplex) name, as specified in parmlib member COUPLE*xx*, is not the same for all of these systems.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 339. DASDVOL NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.

Table 339. DASDVOL NEWLIST: Audit priority values and descriptions (continued)

Priority	Meaning
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

BOX_SERIAL

Text field that describes the serial number and device ID for the DASD unit as described by the Common Device Architecture (CDA) commands. The output field has the format `Man-Fa-Serial-Id`, consisting of a Manufacture ID, Factory ID, Serial number, and Device ID.

Table 340 lists some common device IDs from several manufacturers.

Table 340. Manufacturer Device ID values

Id	Manufacturer
IBM	IBM
AM1	Amdahl
HDS	Hitachi
STK	StorageTek

BOX_TYPE

This text field describes the type serial number for the DASD unit as described by the Common Device Architecture (CDA) commands. The output field has the format '**Type-Mod**', consisting of a disk model and disk type, `3390-06` for example.

COMPLEX

The security complex that contains the system. This value can be taken from the ALLOC COMPLEX parameter or default to a system name.

DEVICE

Repeated text field that describes the device number for the DASD volume in three or four hexadecimal characters. This field is part of the structured repeat-group described with the SYSTEM field.

Note: This field is a text field. If you specify selection criteria using the relational operators (`< > ,<=`, or `>=`), the selection is based on *text* values, not on numerical values.

MOUNTED

This flag field is repeated for each of the target systems to which the DASD volume is attached. It describes whether the current system has mounted the DASD volume. This field is part of the structured repeat group described with the SYSTEM field.

If a system has not mounted a volume (`MOUNTED=NO`), most of the fields in the structured repeat group are blank.

ONLINE

Describes the number of systems on which the current volume has been mounted. That is, the number of times the MOUNTED field is set in the structured repeat group described with the SYSTEM field.

ORG

A number identifying the current entry. Currently, numbering starts at 1, and increases by 1 for each physical DASD volume processed.

Note: The function, format, or value for the ORG field might change. For example, the hardware serial number can change. Do not create reports that depend on the output of this field.

SHARED

This flag field is repeated for each of the target systems to which the DASD volume is attached. It describes whether the current system handles the DASD volume as shared with other systems. This field is part of the structured repeat group described with the SYSTEM field.

The SHARED field can cause either of the following audit concerns to be set:

- If volume is marked shared but is only used on one system, a concern is set because the sharing causes an avoidable performance loss.
- If a volume is not marked shared on all systems that share it, a concern is issued because this configuration can lead to unsynchronized updates and cause a loss of data on the volume.

This field reflects the shared attribute as set in the UCB, *not* as set by the SIMULATE SHARED command.

SMS_MANAGED

This flag field is repeated for each of the target systems to which the DASD volume is attached. It describes whether the current system handles the DASD volume as SMS-managed. This field is part of the structured repeat group described with the SYSTEM field.

SYSTEM

This text field is repeated for each of the target systems to which the DASD volume is attached. It describes the system name. This field is the unique index in the structured repeat group also containing the ATTR, DEVICE, MOUNTED, SHARED, SMS_MANAGED, UNIT, and USE fields. If the MOUNTED attribute is not set (MOUNTED=NO) for any of these repeat-group entries, only the SYSTEM and MOUNTED fields in the repeat group entry are set; all others are left blank.

UNIT

This text field is repeated for each of the target systems to which the DASD volume is attached. It describes the unit type name for the volume on the current system. This field is part of the structured repeat group described with the SYSTEM field.

USE

This text field is repeated for each of the target systems to which the DASD volume is attached. It describes the Mount and Use attributes for the volume on the current system, which determines the type of data set that can be placed on a volume. This field is part of the structured repeat group described with the SYSTEM field. Table 341 on page 1016 lists the values of the USE field.

Table 341. Values for USE field

USE value	Meaning
PRIVATE	The volume is only used for allocation requests specifically using this volume.
PUBLIC	The volume is used for scratch data sets, and for allocation requests specifically using this volume.
STORAGE	The volume is used primarily for non-temporary data sets. It can also be used for scratch data sets and allocation requests specifically using this volume.

Note: The mount use attribute is ignored if the volume is SMS-managed.

VOLSER, VOLUME

The volume serial of the DASD volume.

DB2_REGION: DB2 subsystems

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•		•	•	•	•	•

This section describes the fields for the DB2_REGION NEWLIST. This NEWLIST type lists one entry per active DB2 subsystem for each system for which data is available in allocated CKFREEZE data sets. An entry is uniquely identified by the fields COMPLEX, SYSTEM, and DB2ID.

Field descriptions

The `DB2_REGION NEWLIST` provides the following fields for reporting.

ASID

This field contains the address space ID associated with the DB2 region. The address space ID is a 2-byte hexadecimal number.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 342. DB2_REGION NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CHAROPT

This single character field shows the suffix of the resource classes used by the DB2 RACF security module. Its value is ignored for DB2 subsystems that use classification option (CLASSOPT) 2 for multi-subsystems and for DB2 subsystems that use the default value DSN for the class name root (CLASSNMT).

CLASS_BUFFER_POOL

This field shows the resource class used by the DB2 RACF security module for verification of buffer pool privileges.

CLASS_COLLECTION

This field shows the resource class used by the DB2 RACF security module for verification of collection privileges.

CLASS_DATABASE

This field shows the resource class used by the DB2 RACF security module for verification of database privileges.

CLASS_JAR

This field shows the resource class used by the DB2 RACF security module for verification of Java archive privileges.

CLASS_PACKAGE

This field shows the resource class used by the DB2 RACF security module for verification of package privileges.

CLASS_PLAN

This field shows the resource class used by the DB2 RACF security module for verification of plan privileges.

CLASS_SCHEMA

This field shows the resource class used by the DB2 RACF security module for verification of schema privileges.

CLASS_SEQUENCES

This field shows the resource class used by the DB2 RACF security module for verification of sequences.

CLASS_STOREDPROC

This field shows the resource class used by the DB2 RACF security module for verification of stored procedure privileges.

CLASS_STORGRP

This field shows the resource class used by the DB2 RACF security module for verification of storage group privileges.

CLASS_SYSTEM

This field shows the resource class used by the DB2 RACF security module for verification of system privileges.

CLASS_TABLE_INDEX_VIEW

This field shows the resource class used by the DB2 RACF security module for verification of table, index and view privileges.

CLASS_TABLESPACE

This field shows the resource class used by the DB2 RACF security module for verification of tablespace privileges.

CLASS_USER_FUNCTION

This field shows the resource class used by the DB2 RACF security module for verification of user function privileges.

CLASS_USER_TYPE

This field shows the resource class used by the DB2 RACF security module for verification of user type privileges.

CLASSNMT

This four-character field shows the class name root of the resource classes used by the DB2 RACF security module. The class name root is the middle part of the resource class name, between the prefix and suffix. Its value is ignored for DB2 subsystems that use classification option (CLASSOPT) 1 for single subsystems.

CLASSOPT

This single-digit number field shows the classification option used by the DB2 RACF security module. Possible values are 1 for use of the resource classes by a single DB2 subsystem only, or 2 for shared use of the same resource classes by multiple DB2 subsystems.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

DB2ID

This field shows the DB2 subsystem identification. Maximum length: 4 characters.

GROUP_NAME

This field shows the DB2 group attachment name if the DB2 subsystem is part of a data sharing group. If the DB2 subsystem is not part of a data sharing group, the field is missing (not applicable).

JOBID

This field contains the JES job ID of the DB2 subsystem. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the DB2 subsystem. Maximum length: 8 characters.

LU_NAME

This field contains the VTAM LU-name by which this DB2 subsystem is known. It is also used as the VTAM APPL name. The maximum length is 8 characters.

PC_LX

This 4-byte hexadecimal field shows the linkage index (LX) and program call (PC) number used to connect to the DB2 subsystem.

REGION_USERID

This field contains the userid associated with the DB2 subsystem. Maximum length: 8 characters.

SITE_NAME

This field contains the name by which other systems in the network can recognize the DB2 subsystem. In DB2, this field is also known as the location name. The maximum length is 16 characters.

STEPNAME

This field contains the step name associated with the DB2 region. Maximum length: 8 characters.

SUBSYS_CHAR

This field specifies the console command character that is used to enter commands from a console. Length: 1 character.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

DEFTYPE: user-defined data source

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•		•	•	•	•

Use the `NEWLIST TYPE=`*`deftype`* to specify user-defined files to provide maximum flexibility in reporting on any database or logfile necessary. You can use this `NEWLIST` for defining extra log types or adding lookup data to reports. You must define the *deftype* through a `DEFTYPE` statement. It has few predefined fields.

Field descriptions

The `DEFTYPE NEWLIST` provides the following fields for reporting.

COMPLEX

The security complex to which the file has been assigned. This value comes from the ALLOC COMPLEX parameter.

DDNAME

The DDNAME of the file containing the record.

RECNO

The record number of the current record within its input file (not overall). The RECNO field applies to the number of complete **logical** records within a single input file, counting the first record as 1.

Note: For SELECT/EXCLUDE processing, only the =. <>, and ¬= relational operators can be used.

RECORD

The RECORD field contains a single full record. This field is designed to be used with the DEFINE command in combination with field-value manipulation functions. See "DEFINE" on page 750 and "Field value manipulation" on page 760.

Note: This field has format ASIS by default, which has been built specifically to keep trailing spaces intact. This format is also inherited by fields defined with RECORD as base. If trailing spaces need to be trimmed, use the overriding format CHAR can be used.

RECORDLENGTH, RECORD_LENGTH

This field describes the length of the DEFTYPE record in bytes, excluding the RDW. The given length is the one of the **logical** record.

DSN: Data Set Names (non-VSAM)

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The DSN NEWLIST (NEWLIST TYPE=DSN) describes the data set names on the system, annotated with protection information. This NEWLIST requires input source files that include one or more CKFREEZE files with data set information. Each record in this NEWLIST represents a data set name, including references without an actual data set name. A record is uniquely identified by the fields SYSTEM, COMPLEX, DSN_TYPE, DSNAME, VOLUME, CATALOG, CATALOG_VOLUME, REAL_DSN and REAL_VOLUME. For information about these fields, see "Field descriptions."

Note: The present version only reports non-VSAM data sets (DSN_TYPE=' nvsam'). It does not report non-VSAM aliases. It does not relate migrated data set names to REAL_DSN and REAL_VOLUME. It does not support GDGs.

Field descriptions

The DSN NEWLIST provides the following fields for reporting.

ALIAS_RELATE

Contains the catalog name related to the CATALOG_ALIAS used for this data set. That is, the catalog the data set is found in using a standard search, if any. For a symbolic relation, this field shows the symbolic name. See ALIAS_RELATE_EFFECTIVE, VIA_SYMBOLIC_RELATE.

ALIAS_RELATE_EFFECTIVE

Contains the catalog name related to the CATALOG_ALIAS used for this data set. That is, the catalog the data set is found in using a standard search, if any. For a symbolic relation, this field shows the resolved name. See ALIAS_RELATE, VIA_SYMBOLIC_RELATE.

BOX_SERIAL

Describes the volume serial number and device ID for the DASD unit where the data set is stored. This field can be used to disambiguate between DASD volumes with the same VOLSER. See also "BOX_SERIAL field for DASDVOL report" on page 1014.

CATALOG

Contains the name of the catalog the data set name is in.

CATALOG_ALIAS

Contains the catalog alias that is used for this data set name in a standard search, if any alias is used. See ALIAS_RELATE, ALIAS_RELATE_EFFECTIVE, VIA_SYMBOLIC_RELATE.

CATALOG_VOLUME

This field contains the volume where the catalog resides that contains an entry for this data set.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

Contains the name of the security complex. This value can be taken from the COMPLEX= keyword on an explicit ALLOC statement or it can default to a system name.

DSN, DSNAME

Contains the data set name. This value might only be a reference, a catalog entry for example. See REAL_DSN.

DSN_TYPE

Contains the data set type. Currently always 'nvsam' for non-VSAM.

IN_CONNECTED_CATALOG

Flag field that indicates if the data set is cataloged in a user catalog connected to the master catalog.

IN_DIRECTED_CATALOG

Flag field that indicates if the data set is cataloged in a catalog that is not used in a standard search.

IN_MASTER_CATALOG, IN_MCAT

Flag field that indicates if the data set is cataloged in the master catalog of this SYSTEM.

IN_VTOC

Flag field that indicates if the data set occurs in the *Volume Table Of Contents* for VOLUME.

IN_VVDS

Flag field that indicates if the data set occurs in the *VSAM Volume Data Set* of VOLUME. A non-VSAM data set occurs in the VVDS if it is SMS-managed.

IS_MIGRATED

Flag field that indicates if the data set name references a migrated data set.

IS_MOUNTED

Flag field that indicates if VOLUME is mounted.

PROFILE

The RACF profile protecting this data set (RACF systems only). See RESOURCE.

QUAL

Contains the first qualifier of the resource name checked for this data set as translated by ICHNCV00 and ICHCNX00. See RESOURCE.

QUAL_IS_DATASET_PROFILE

Flag field that indicates if a profile exists in the RACF database of the form *qual.*** or *qual.*.***, where *qual* is the first qualifier of the resource name checked for this data set.

QUAL_IS_GROUP

Flag field that indicates if the first qualifier of the resource name checked for this data set matches a group in the security database.

QUAL_IS_USER

Flag field that indicates if the first qualifier of the resource name checked for this data set matches a user ID in the security database.

REAL_DSN, REAL_DSNAME

Contains the real data set name. This value is equal to the DSNAME if the data set occurs in the VTOC. Otherwise, the value is missing.

REAL_VOLUME

Contains the real volume for the data set. The value is the same as the VOLUME if the data set occurs in the VTOC. Otherwise, the value is missing.

RESOURCE

Contains the resource name checked for this data set as translated by ICHNCV00 and ICHCNX00.

SENSITIVITY

Contains the data set sensitivity type for sensitive data sets. See the SENSITIVITY field description in "SENSITIVITY" on page 1258 for the sensitive data sets automatically recognized.

SYSTEM

Contains the name of the (viewpoint) system. For MVS systems, this value is the SMF system ID. The default field length is the field is 8 characters for compatibility with other NEWLISTs.

UNITTYPE

This field contains the device type for the data set volume.

VIA_SYMBOLIC_RELATE

Flag field that indicates the CATALOG_ALIAS used for this data set in a standard search (if any) has a symbolic relation. See ALIAS_RELATE, ALIAS_RELATE_EFFECTIVE.

VOLUME, VOLSER, VOL

Contains the data set volume. This value might only be a reference, a catalog entry for example. See REAL_VOLUME.

DSNT: RACF Data Set Name Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The DSNT NEWLIST (NEWLIST TYPE=DSNT provides information about the in-storage Data Set Name Table per system. This table is built as the result of the contents of the ICHRDSNT module at IPL, subsequent RVARY commands, and possibly operator replies. Unless otherwise stated, all fields can be used for SELECT or EXCLUDE processing as well as in the following output commands: LIST, SORTLIST, DISPLAY, and SUMMARY. The DSNT NEWLIST generates one entry per in-storage Data Set Name Table entry per system. A unique key for this NEWLIST is the SYSTEM ORDER field.

Field descriptions

The DSNT NEWLIST provides the following fields for reporting.

ACTIVE

Active flag, indicating whether this data set is currently active.

ATTR

A string listing the RACF data set attributes, with a text representation of all flag fields that are set. The following table shows the flags used to make up this string.

Flag	String entry	Meaning
ACTIVE	Act	Active data set
CMS	CMS	Data set in CMS minidisk format
DATABUF	Databuf	Data block buffering active
	DataShare	Data sharing mode active, all other members in IRRXCF00 in data sharing mode or read-only.
	DataShareR/O	Read-only mode active, all other members in IRRXCF00 in data sharing mode or read-only.
	DataShareTrn	Transition mode, will be in data sharing or read-only mode after connect service completes.
MSTR	Mstr	Master data set
PRIM	Prim	Primary data set
RDS	RDS	Restructured data set
SHR	ShrDASD	Master data set is on shared DASD. ICB is read often.
STAT	Stat	Statistics are updated by RACINIT

BUFNO

The number of resident data blocks in (E)CSA. This value is a number in the range of 0 - 255. Higher numbers indicate more storage and potentially better performance. If the installation has not provided an ICHRDSNT module, RACF

uses 10 resident data blocks when sysplex communication has not been enabled. If sysplex communication has been enabled, RACF enforces a minimum value of 50 resident data blocks.

CMS

This flag indicates whether the data set is in CMS minidisk format.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value is taken from the `ALLOC COMPLEX` parameter or default to a system name.

DB, SEQNO

Database sequence number. This number is referred to by the Range Table, which can be displayed with the `NEWLIST TYPE=RRNG`.

DSN, DATASET

Data set name for this database sequence number. This value can be empty if no data set has been defined for a specific backup or sequence number, or if a data set has been made inactive.

MSTR, MASTER

Master data set flag. If this flag is set, this data set is the master data set. The master data set is the data set from which the system-wide options are read from the first block in the data set (the Index Control Block or ICB) during IPL.

ORDER, ORG

The original order (entry number) of this data set entry in the Data Set Name Table. The first entry in the table has ORDER=1.

PRIM

Primary data set flag. If this flag is set, this data set is a primary data set (as opposed to a backup data set). More I/O is performed on a primary data set.

The first primary data set is considered to be the master data set, unless it is set to an asterisk (*) in load module ICHRDSNT. In this case, the operator is prompted during initialization to supply the data set name. The PRIM field reflects the actual data set name in use, whether supplied at IPL, or changed by an RVARY command.

RECTRK

The number of physical blocks per DASD track.

SEQNO

An alias of `DB`. See DB, SEQNO.

SHR, SHARED

Shared flag indicating whether this database is shared with other (MVS or VM) systems. This value is obtained by RACF from the characteristics of the DASD device on which the RACF database is located. If RACF is not activated in sysplex data-sharing mode, the `SHR=YES` results in RACF frequently reading the

Inventory Control Block (ICB) to check for updates made by another system. If RACF is activated in sysplex data-sharing mode, the SHR value is irrelevant.

STAT, STATS, INITSTATS

Indicates if statistical updates to RACF profiles are reflected in the RACF backup data base. Statistics in RACF profiles exist as RACINIT statistics–also known as LOGON statistics–as well as discrete PROFILE access statistics. Maintenance of these statistics is controlled by SETROPTS settings in combination with the installation provided ICHRDSNT module. The STAT flag only reflects the ICHRDSNT-related setting. The SETROPTS settings are controlled by the INITSTATS and the STATISTICS(*classname*) settings.

If RACINIT statistics are to be maintained, RACF sometimes ignores the STAT flag to reliably support the revoke of inactive users.

SYSTEM

The name of the system. For MVS systems, this value equals the SMF system ID. The field length is 8 characters for compatibility with VM systems.

VOLUME, VOLSER, VOL

DASD volume serial for this data set.

DYNEXIT: System Exits

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The DYNEXIT NEWLIST (NEWLIST TYPE=DYNEXIT) provides information about the dynamic exit routines. For each system, this NEWLIST generates one entry per defined dynamic exit. In general, an entry is uniquely identified by the fields SYSTEM and EXITNAME.

Field descriptions

The DYNEXIT NEWLIST provides the following fields for reporting.

ABENDCONSEC

The ABENDNUM and ABENDCONSEC fields indicate how the system handles the abnormal ending of an exit routine. The ABENDCONSEC field indicates whether abnormal endings of an exit routine are counted consecutively (ABENDCONSEC=YES) or cumulatively (ABENDCONSEC=NO).

For more details, see the z/OS internet library. Find the z/OS information center for your z/OS version and search for the ABENDCONSEC field.

ABENDNUM

The ABENDNUM and ABENDCONSEC fields indicate how the system handles the abnormal ending of an exit routine. The ABENDNUM field specifies the number of abnormal endings that can occur before the exit routine becomes inactive. An inactive exit routine is associated with an exit but is not called.

For more details, see the z/OS internet library. Find the z/OS information center for your z/OS version and search for the ABENDNUM field.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 343. DYNEXIT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

ACTIVE#

Contains the number of active exit routines for the exit point.

AMODE

Contains the required addressing mode for exit routines. Possible values are *24*, *31*, or *Def*. The value *Def* indicates that the exit routine takes control in the AMODE that was defined for the load module for the exit routine at the time it was created.

ANYKEY

Flag field that indicates if an exit routine can be called in any key. The field requires that the exit routines are reentrant, and only applies to exit routines that are called in fast path mode.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

Specifies the security complex that contains the system. This value can come from the `ALLOC COMPLEX` parameter or a default determined by the application.

DESC, DESCRIPTION

A string of up to 45 characters that explains the exit function. The description is taken from an internal knowledge base.

EXECKEY

Shows the storage key and execution key that is used when the exit module is called. This field is only present for modules that are defined for a dynamic exit point. These keys are specified by the application when the dynamic exit point is defined. The field only applies to non-reentrant modules and to modules called in fast path mode.

EXITNAME

Describes the full name of the dynamic exit as specified by the `EXITNAME` parameter in the `PROGxx` member in `PARMLIB`.

EXPLICIT
Flag field that indicates if the exit module has been defined. This field is only present for modules that are defined for a dynamic exit point.

YES indicates that the exit module has been defined. This value corresponds to the value E for the defined status as reported by the D PROG operator command.

NO indicates that the exit module has not been defined. This corresponds to the value I for the defined status as reported by the D PROG,EXIT operator command.

FASTPATH
Flag field that indicates if the exit routine can be called in fast path mode. When the exit routine is called in this mode, it provides reduced recovery, and the exit routine runs in the state and key of the caller. Fast path must also be explicitly requested by the exit caller to be used.

INACTIVE#
Contains the number of added, but inactive exit routines for the exit point.

RENT_REQ
Specifies whether exit routines to be added to the exit are required to be reentrant.

SINGLEMODULE
Flag field that indicates that only a single module can be associated with the exit point at a time.

SYSTEM
Returns the name of the system. For MVS systems, this value is equal to the SMF system ID. The field is eight characters long.

EXIT: System Exits

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The EXIT NEWLIST (NEWLIST TYPE=EXIT) provides information about system exits. For each system, this NEWLIST generates one entry per exit or table. However, some exits are taken from a directed load, such as STEPLIB. When more than one data set with the exit is found, the exit is reported multiple times. For implicit dynamic exits, the associated modules might not be included in the EXIT NEWLIST report. The program does not attempt to locate these modules, and they are not listed as exit routines.

In general, a unique key for an entry in the EXIT NEWLIST is SYSTEM PROGRAM JOBNAME ADDRESS. For dynamic exits, the unique key also includes the EXITNAME field.

Field descriptions

The Exit NEWLIST provides the following fields for reporting.

ACTIVE
Flag field that indicates if a module is active. This field is only present for modules that are defined for a dynamic exit point.

YES indicates that the module is active.

NO indicates that the module is defined as INACTIVE or that it has become inactive because of an ABEND.

ACTIVE_EFFECTIVE
Flag field (YES or NO) that can be used to determine if a module is called as a dynamic exit routine. This field is only present for modules that are defined for a dynamic exit point. It is the logical combination of the ACTIVE and EXPLICIT fields.

ADDRESS

This field contains the address of the exit or table. For exits, this is the *entry point* of the exit, for example the address used by MVS to branch to this exit routine. For tables, this is the start address of the table.

AMODE

This field contains the addressing mode of the exit or table. This will be **24**, **31**, or **64**.

ANYKEY
Flag field (YES or NO) that indicates if an exit routine can be called in any key. This field is only present for modules that are defined for a dynamic exit point. This field only applies to exit routines that are reentrant.

APPL

Indicates the application or subsystem owning the exit or table. The following table shows the exit types supported by the current version, and the resulting values of the APPL field:

Table 344. Exit type and associated APPL field value

Application/Subsystem	APPL value
ACF2	ACF2
CA-1	CA1
dynamic exit facility	dynamic
HSM	HSM
I/O appendage	IOAPP
JES2	JES2
MPF	MPF
RACF	RACF
SMF	SMF
TSO	TSO
WTO	WTO

AT

This field contains a short description of the exit program name, module name, and offset, in the format described in the following table. The format is derived from the exit's entry point.

Table 345. AT description format

AT format	Minor/Major EP	Offset zero
Module	Major	Yes
Module+offset	Major	No

Table 345. AT description format (continued)

AT format	Minor/Major EP	Offset zero
Program in Module	Minor	Yes
Program+offset in Module	Minor	No

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. Audit concerns are described in the following list. The AUDITCONCERN field can contain one or more concerns separated by commas.

- Exit in writable common storage

  The exit code resides in writable common storage; any user can alter the exit.
- String scan hit

  The SCAN_STRING field registered a hit: a user-defined string was found in the exit code.
- SVC scan hit

  The SCAN_SVC field registered a hit: a user-defined SVC call was found in the exit code.
- Instruction scan hit

  The SCAN_INSTR field registered a hit: one or more specific instructions scanned for were found in the exit code.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 346. EXIT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

CONTENT, CONTENTS

This field contains up to the first 256 bytes of the contents of the exit or table, which usually include the eye catcher. The default output length of this string is 59 characters (containing the first 59 bytes of the exit). In the default output

format, the readable text from the contents is shown; the non-printable parts of the contents have been replaced by one or two dots.

DESC, DESCRIPTION

A string of up to 45 characters explaining the function of the exit or table. The description is taken from an internal knowledge base.

EXECKEY

This field shows the storage and execution key that is used when an exit module is called. This field is only present for modules that are defined for a dynamic exit point. The key values are specified by the application when the dynamic exit point is defined. The field only applies to non-reentrant modules and to modules called in fast path mode.

EXITNAME

If the current exit is dynamic, this field describes the full name of the dynamic exit, as specified by the EXITNAME parameter on the PROGxx member of SYS1.PARMLIB. If the exit is not a dynamic exit, this field is blank.

EXPLICIT

Flag field that indicates if the module has been added to a defined exit point. This field is only present for modules that are defined for a dynamic exit point.

YES indicates that the module has been added to a defined exit point. This value corresponds to the value E for the defined status as reported by the D PROG operator command.

NO indicates that the module has been added, but the exit point has not been defined. This corresponds to the value I for the defined status as reported by the D PROG,EXIT operator command.

FILTER_JOBNAME

Shows the `JOB` filter pattern used to control if this module is started. This field is only present for modules that are defined for a dynamic exit point. This field is empty if the `FILTER_TYPE` is not *Jobname*.

FILTER_STOKEN

Shows the Address Space `STOKEN` filter used to control if this module is started. This field is only present for modules that are defined for a dynamic exit point. The field is empty if the `FILTER_TYPE` is not *SToken*.

FILTER_TYPE

Shows the type of filter defined for the exit module. This field is only present for modules that are defined for a dynamic exit point. Filtering can be done by `jobname` or by active primary address space (`stoken`). Jobname filtering can be specified either using the API interface or the `SETPROG` operator command. `STOKEN` filtering can only be specified using the API interface. This field can return the following values for the FILTER_TYPE: *Jobname*, *SToken*, or blank if filtering is not active.

JOBNAME

If the exit resides in PVT or EPVT, this field contains the jobname of the address space in which the exit is located. If the exit lies in common storage (and is available to all address spaces), this field is left blank.

KEY

This field contains the storage protection key of the exit or table, if the exit or table is in CSA, ECSA, SQA, or ESQA.

A key of 8 is a serious cause for concern; any user might be able to change the exit. A key of 9 to 15 is a minor cause for concern; only users running in that key will be able to change the exit, while keys 9 to 15 can normally only be used by controlled applications, when running programs from APF libraries. An exception goes for ADDRSPC=REAL, see 1451.

LENGTH

This field contains the length of the program/module the exit or table is part of, if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA). If CKFREEZE contains sufficient information, it might also be filled in if the residency is a server address space private area (PVT, EPVT). The length is approximated as the length up to the end of the module, or the length up to the next entry point.

MODULE

This field contains the major entry point name of the module in which the table or exit is located, if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA). If CKFREEZE contains sufficient information, it might also be filled in if the residency is a server address space private area (PVT, EPVT)

OFFSET

This field contains the offset between the program's entry point and the exit or table address, if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA). If CKFREEZE contains sufficient information, it might also be filled in if the residency is a server address space private area (PVT, EPVT). The offset is calculated from the previous entry point, and is zero if the address is located at a minor or major entry point.

PARAM

Shows an optional input parameter that is passed to the exit routine. This field is only present for modules that are defined for a dynamic exit point. The value returned corresponds to the value shown when using the `DIAG` option of the `D PROG,EXIT` operator command. By default, the `PARAM` field is shown as 16 hex digits, while the `D PROG,EXIT` operator command tries to show the field as printable characters. The PARAM field is only present when using a `CKFREEZE` file created by CKFCOLL V 1.12 or later, running on a z/OS system, V 1.12 or later.

POSITION

Shows the sequence number in which the module is called for the exit point. This field is only present for modules that are defined for a dynamic exit point. The POSITION field is only valid when using a `CKFREEZE` file created by CKFCOLL V 1.12 or later. For `CKFREEZE` files created using a earlier release level of CKFCOLL, the value zero is suppressed.

PROGRAM

Depending on the exit type, this field contains one of the following types of data:

1. The documented name of the exit. This does not need to correspond to the actual module name (because this reflects an exit address in a control block). This happens for ACF2, JES3, and RACF exits. For in-storage tables that represent the combination of two or more modules, a name is constructed with a lowercase character in the name, for example, ICHRRCDx is the name that is constructed for load modules ICHRRCDE and ICHRRCDX.
2. A documented exit name that is also the actual load module name. This happens e.g. for some DFSMS, MVS, and VTAM exits.

3. The name according to some descriptor control block (for example, for JES2 , CA-1, TSO, and dynamic exits), where the name does not need to correspond to the actual module name, but often does if the exit has not been front-ended.

For the actual load module name associated with the exit address used by z/OS, see the field AT.

RESULT

This field is always blank for tables; for exits, it contains a string containing the result of a disassembly of the exit. Set to 'RC=**n**' if the exit has a fixed return code of 0, 4 or 8; empty otherwise. For the password encryption exit ICHDEX01 or ICHDEX11, the string is set to 'RC=**x: comment**', where 'comment' describes the effect of the return code. Possible values of RESULT for ICHDEX01 are documented in the following table.

Table 347. RESULT values for password encryption exit ICHDEX01

Return code	RESULT value
0	RC=0: Installation-defined encryption
4	RC=4: Force masking, no DES encryption
8	RC=8: Force DES encryption, no masking

SCAN_INSTR

This field describes the result of an *instruction scan* performed on the full exit code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter. The instruction scan is performed on the full length of the exit (not just on the eye catcher), and checks for suspicious instructions in the code.

Note: You should use the contents of this field as a warning, not as a certainty. The instruction scan might cause false alarms, and can also be fooled to miss certain instructions. You should always review the source code of suspicious modules.

When used for SELECT/EXCLUDE processing, you can use SELECT SCAN_INSTR or SELECT SCAN_INSTR=ANY to select routines in which *any* specified instruction was found; use SELECT SCAN_INSTR=NONE to select routines in which no specified instructions were found. In addition, you can select routines containing any of the specific instructions listed in the following table, for example, SELECT SCAN_INSTR=(FAKEAPF,FAKESPEC).

Because many suspicious instructions can be found within a single module, the default output of this field is in a condensed format; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 9, for example SCAN_INSTR(EXPLODE,9). The following table lists the SCAN_INSTR values that can be used for SELECT/EXCLUDE processing; the condensed output; the exploded output; and the meaning.

Table 348. SCAN_INSTR values available for SELECT/EXCLUDE processing

Select/Exclude	Condensed	Exploded	Meaning
BYPASS BYPASSSAF	.B.....	BypassSAF	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	FakeAPF	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	FakeOper	Set operations authority

Table 348. SCAN_INSTR values available for SELECT/EXCLUDE processing (continued)

Select/Exclude	Condensed	Exploded	Meaning
FAKEPRIV	......P	FakePriv	Set privileged/trusted authority
FAKESPEC	....S..	FakeSpec	Set special authority
KEYZERORB	...0...	KeyzeroRB	For an SVC: modify caller's RB to key-zero
MODESUPRB	..M....	ModeSupRB	For an SVC: modify caller's RB to supervisor mode

Note: The values printed by the SCAN_INSTR field are subject to change. Do not write applications that are dependent on the output of this field.

SCAN_STRING

This field describes the result of a *string scan* performed on the full exit code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSTR arguments set. The string scan is performed on the full length of the exit (not just on the eye catcher), and checks for user-specified strings in the code.

The value of this field is set to **Yes** if a matching string was encountered in the code; **No** if no string was found; the field is left blank if no string scan was performed.

SCAN_SVC

This repeated field describes the result of an SVC *scan* performed on the full exit code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSVC list of SVC numbers set. The SVC scan is performed on the full length of the exit (not just on the eye catcher), and checks for user-specified SVC calls in the code.

Note:

You should use the contents of this field as a warning, not as a certainty. The SVC scan might cause false alarms, and can also be fooled to miss certain SVC calls. You should always review the source code of suspicious modules.

The value of this field has the format *num*: *description* if the SVC scanned for was one of the first seven specified in zSecure Collect. If any of the other SVCs scanned for was encountered, this field has the value *Other*.

SUBPOOL

This field contains the storage area subpool of the exit or table, if the residency is in CSA, ECSA, SQA, or ESQA.

SUBSYS, SUBSYSTEM

This field contains the name of the subsystem owning the exit or table. In the current version of Security zSecure, this field will only be set for JES2 exits (APPL=JES2), and be left blank otherwise. The SUBSYS field describes the actual JES2 name. For more information on the subsystem, use the NEWLIST TYPE=SUBSYS described in section 'SUBSYS MVS Subsystems'.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. This field length is 8 characters to cater to VM systems.

WHERE

A string indicating the virtual storage area where the exit or table resides. Possible WHERE values and their meaning are documented in the following table; areas starting with an E reside above the 16 MB line in virtual storage.

Table 349. WHERE values and descriptions

WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

FIELD: Field Properties per NEWLIST type

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The `FIELD NEWLIST` (`NEWLIST TYPE=FIELD`) lists fields for all Security zSecure report or `NEWLIST` types with most of their properties like default output length, format, headers, and so on. For some NEWLIST types, additional fields are available but not present in `TYPE=FIELD`. In that case, a separate `NEWLIST` type is available to list the additional fields defined in a security database. For RACF profiles (`NEWLISTYPE=RACF`) use `TYPE=TEMPLATE` to see the fields defined through RACF database templates. The fields listed in the FIELD NEWLIST are similar to these other `NEWLIST`s, but `TYPE=FIELD` lists pseudo-fields that are not available directly in the security database. In the ISPF user interface, the result can be displayed through the FIELD primary command, which imbeds the CARLa script `C2RDFLD`. This script also provides sample CARLa statements for using the `FIELD NEWLIST`.

Field descriptions

You can use the following fields to select and create audit reports for System settings.

ADVERTIZE

Flag indicating whether the field should be advertised. This is set to NO for fields where a better alternative is available, and for fields that are not available for either direct selection or direct output. It is up to the CARLa writer to decide whether to include those or not. The FIELD primary command only shows fields that should be advertised.

BASE

This indicates whether the field value is derived from another field value (but not exactly the same, like it would be for an alias name - alias names are not available in TYPE=FIELD). Maximum length is 24 characters, default length is 8 characters, If present, the field inherits some properties from the base field. For example, which segment should be read to be able to do a lookup, and which resource name should be used for FIELD scoping checks.

CASESENSITIVE

Flag indicating whether user input on a modifiable field is case-sensitive. It is off if the field is not modifiable.

COMPARE_USAGE

This flag field determines whether the specified field can be used in a comparison process as specified in a COMPAREOPT COMPARE statement.

COMPARE_USAGE_BY

This flag field indicates whether the specified field is included in the default BY specification which specifies the key of the record to be used in a comparison process. For more information, see the COMPAREOPT statement.

COMPARE_USAGE_COMPARE

This flag field indicates whether the specified field is part of the default COMPARE specification. For more informations, see the COMPAREOPT statement.

COMPLIANCE_IMPROVEMENT

Indicates whether a change in the value of a field resulted in increased or decreased security compliance. Table 350 lists the possible field values. This field is included in the COMPARE_CHANGES field that reports the changes detected during a comparison process. Use input and output formats to determine whether the compliance value information is included in the comparison data reported by COMPARE_CHANGES. For more information, see “COMPARE processing output formats: Formatting COMPARE_CHANGES results” on page 829.

Table 350. Compliance Improvement - possible field values

Compliance value	Meaning
Increasing	The change detected for the specified field increased the security compliance. In reports and displays, changes that result in increased compliance have a + indicator.
Decreasing	The change detected for the specified field decreased security compliance. In reports and displays, changes that result in decreased compliance have a - indicator.
Missing	The current NEWLIST is not the result of a comparison operation.

DESCRIPTION

Field prefix header. Maximum length is 29 characters. You get this by using the PREFIX modifier on a field on a LIST, SORTLIST, DISPLAY, SUMMARY, DSUMMARY, or DEFINE AS statement, or HEADER=PREFIX on a NEWLIST, BUNDLE, PRINT, or OPTION statement.

DESCRIPTION_ORIG

This field shows the original (English) default field prefix header (field label). The maximum length is 29 characters.

FIELD

Field (variable) name. Maximum length is 24 characters. This is the built-in field name you can specify on a LIST, SORTLIST, DISPLAY, SUMMARY, DSUMMARY, SELECT, EXCLUDE, or DEFINE AS statement behind a NEWLIST statement with the appropriate type (see field NEWLIST_TYPE).

FIELD_TAG

IBM Security zSecure internal number identifying built-in fields within the NEWLIST type.

FORMAT

Output format name. Maximum length is 16 characters.

HEADER

Default column header when the field is used on SORTLIST, DISPLAY, SUMMARY or DSUMMARY.

HEADER_ORIG

This field shows the original (English) default field column header. The maximum length is 48 characters.

HELP_PANEL

Field-level help panel name. Maximum length is 8 characters. This is the help panel that will be displayed when pressing HELP while the cursor is on the field value or its column header or prefix header in an ISPF display (caused by a DISPLAY or DSUMMARY statement listing the field in FIELD).

HORIZONTAL

Repeating values must be displayed horizontally. See also “HORIZONTAL” on page 805.

LENGTH

Default output length.

LENGTH_ORIG

This is a decimal number that shows the original (English) default field output width. The field length is 6.

LOOKUPONLY

Flag indicating that the field can only be used as a lookup target field (for example, the right side of a lookup operator). This flag is only present for a number of TYPE=RACF fields.

MAXIMUM_LENGTH

Field indicating maximum length on input. If omitted this is taken to be the same as the output length on a display and subject to a general limit on SELECT.

MODIFIABLE

Flag indicating whether field might be modified on the display if an appropriate product is installed and not disabled. In addition, actual modifiability might be restricted by insufficient OS or security system software and database levels.

NEWLIST_ABBREV

A 2-character key for NEWLIST type as used in CKR.ACTION resource names. See also *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

NEWLIST_TAG

IBM Security zSecure internal number identifying the NEWLIST type.

NEWLIST_TYPE

A NEWLIST type. The maximum length is 24 characters. For the list of NEWLIST types see "Overview of NEWLIST types" on page 850. NEWLIST types starting with R_ are an abbreviated form of REPORT_.

REPEATED

Flag indicating whether this field can return more than one value in a single record.

RESTRICT

Field that contains output and scope restrictions. It is a character field with one or more strings. All of those restrictions except 'Sensitive' are only returned if running in restricted mode. It is currently only filled in for NEWLIST_TYPE RACF.

Auditor
In restricted mode, limit display to system-wide auditors and group auditors.

Field
In restricted mode, limit display to people with FIELD authority.

CKGownr
In restricted mode, the field is visible for objects in the CKGRACF scope with READ access. See "Scope profiles" on page 1563 to see how this scope is defined.

Owner
In restricted mode, the field is visible when the object is in the RACF or CKGLIST scope of the user. The RACF scope includes system-special, system-auditor, system-operations, group-special, group-auditor, group-operations, and ownership scope as appropriate for the RACF class.

Read
In restricted mode, the field is visible when the user has READ access or higher on the object.

Repeat
In restricted mode, the individual repeat group entries are subject to individual scope checks.

Sensitive
The field contains sensitive data like passwords or encryption keys that should not be stored outside the security database or printed.

SUBSELECT

This (repeated) field can contain the name of one or more subselect groups (ACL, CONNECTS, or USR). This means the field can only be used in a DEFINE SUBSELECT statement, unless it is also present in TYPE=TEMPLATES.

TRANSLATED

This boolean flag indicates whether the LANGUAGE statement contains a FIELD clause for this field. The field length is 3.

WRAP

Field must be wrapped to the next display line(s) if the output area is not wide enough. See "WRAP" on page 802.

FIELD_OVERRIDE

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

FIELD_OVERRIDE NEWLIST enumerates the output fields encountered in this run that have field-level overrides. The FIELD_OVERRIDE records list original and translation properties for each visible field or output string occurrence on LIST, SORTLIST, DISPLAY, SUMMARY, or DSUMMARY specifications where a length, header, or prefix header property was specified in the CARLa TYPE=FIELD_OVERRIDE.

The default toptitle for this NEWLIST is: NEWLIST FIELD OVERRIDES. The key for a FIELD_OVERRIDE record is NEWLIST_TYPE NEWLIST_NAME SRCEDDN SRCEMEM SRCELINE ORDER FIELD OCCURRENCE.

Field descriptions

The FIELD_OVERRIDE NEWLIST provides the following fields for reporting.

DESCRIPTION

This field shows the original (English) default field prefix header (field label). The maximum length is 29 characters.

DESCRIPTION_ORIG

This field shows the original (English) default field prefix header (field label). The maximum length is 29 characters.

FIELD

This is the field name as it occurs on the LIST family statement, except that for TYPE=RACF alias field names might have been converted to canonical field names. The maximum length is 24 characters.

HEADER

This field shows the final (optionally translated) column header as it is used. It is empty if a prefix header was used. The maximum length is 48 characters.

HEADER_ORIG

This shows the column header as implied by the LIST family command. It is empty if a prefix header was used. The maximum length is 29 characters.

LANGUAGE

A three character abbreviation that identifies the target language for the translated version of the output from this NEWLIST.

LENGTH

This is a decimal number that shows the original (English) default field output width. The field length is 6.

LENGTH_ORIG

This is a decimal number that shows the original (English) output width (the CARLa length override if present). The field length is 6.

NEWLIST_NAME

The NEWLIST_NAME field shows the NAME passed on the NEWLIST statement, optionally suffixed with `.DISPLAY` if the NEWLIST contains a DISPLAY or DSUMMARY statement, as opposed to only a subset LIST, SORTLIST, and SUMMARY. This field has a maximum length of 16.

NEWLIST_TYPE

The NEWLIST type in character format. This field has a maximum length of 24.

OCCURRENCE

This field displays a number 1 for the first occurrence of a field in the CARLa input, and one higher for each subsequent occurrence. The field length is 2.

ORDER

This field displays a number reflecting the order of the fields as encountered in the CARLa input. The field length is 5.

SRCEDDN

Contains the ddname where the field was encountered. The field length is 8.

SRCELINE

Contains the ddname where the field was encountered. The field length is 8.

SRCEMEM

Provides the member name where the field was encountered, if the ddname is not unique). The field length is 8.

VAL

Shows the final string value after translation. The maximum length is 29 characters.

VAL_ORIG

This shows the original string value as it occurred on the CARLa LIST family command. The maximum length is 29 characters.

IMS_PSB: IMS program specification blocks

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

This section documents the fields for the NEWLIST TYPE=IMS_PSB. This NEWLIST type lists one entry per active IMS program specification block (PSB) for an IMS subsystem in each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, JOBNAME. and PSBNAME.

Field descriptions

The IMS_PSB NEWLIST provides the following fields for reporting.

ASID

This field contains the address space ID associated with the IMS subsystem. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 351. IMS_PSB NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CLASS

This field specifies the resource class used to secure the IMS PSB (for example, IIMS). Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

IMSID

This field specifies the IMS subsystem identification of the IMS subsystem where the IMS transaction is run. Maximum length: 8 characters.

JOBID

This field contains the JES job ID of the IMS subsystem. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the IMS subsystem. Maximum length: 8 characters.

PSBNAME

This field specifies the program specification block (PSB) name. Maximum length: 8 characters.

QUALIFIED_RESOURCE

This field specifies the qualified resource name. It is the concatenation of the RESOURCE_LOCATION and the RESOURCE separated by a colon, for example: IPO1.IMS.IMS10CR1.PSB:DFSSAM04. Maximum length: 44 characters.

RACF_ACL

This repeated field displays the access and conditional access lists of a profile. This field can be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands only. The display contains userid, access, ACL id, conditional class, and conditional profile name. The default output length is 45 characters, but the profile name can be up to 255 characters so the maximum output length of RACF_ACL is 290 characters.

Use the EXPLODE output modifier for a complete access list including access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE. You can use the UNIVERSAL modifier to force collection of all relevant data. The SCOPE modifier extends administrative access control to the modifiers EXPLODE, RESOLVE, and EFFECTIVE. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_CLASS

This field contains the resource class of the profile that protects the resource. The resource class can be a member class or a grouping class. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 8 characters.

RACF_PROFILE

This field contains the name of the profile that protects the resource. The profile can be a member class profile or a grouping class profile. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 13 characters.

RACF_UACC

This field contains the effective universal access authority (UACC) to the program. The UACC is determined from all grouping and non-grouping resource profiles that describe the program. Field values: NONE, READ, EXECUTE, UPDATE, CONTROL, or ALTER.

RESOURCE

This field specifies the resource name used to secure the IMS program specification block (PSB). Maximum length: 246 characters. Default length: 17 characters.

RESOURCE_LOCATION

This field indicates the environment where the resource is relevant. This field is the concatenation of several fixed strings, fields, and lookups, such as *system*.IMS.*jobname*.PSB. An example is IPO1.IMS.IMS10CR1.PSB. Maximum length: 21 characters.

STEPNAME

This field contains the step name associated with the IMS subsystem. Maximum length: 8 characters.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. This field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

TRANSACTION

This is a repeat field that shows the transactions that reference the IMS program specification block (PSB). Maximum length: 8 characters.

VTAM_APPLID

This field specifies the VTAM application identifier (APPLID) for this IMS subsystem. Maximum length: 8 characters.

IMS_REGION: IMS subsystems

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•		•	•	•	•	•

This section documents the fields for the NEWLIST TYPE=IMS_REGION. This NEWLIST type lists one entry per active IMS subsystem for each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, and JOBNAME.

Field descriptions

The IMS_REGION NEWLIST provides the following fields for reporting.

ASID

This field contains the address space ID associated with the IMS subsystem. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field as a programming interface. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 352. IMS_REGION NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CLASS_APSB

This field shows the SAF resource class used for APSB security if APSB security is active. For details, see the SEC_ODBA field. This is the same resource class that was previously used for AGN security. APSB security is used for CPI-C and Open Data Base Access (ODBA) applications. The default class used by IMS for APSB security is AIMS. Maximum length: 8 characters.

CLASS_CMD

This field shows the SAF resource class used for IMS commands if security is activated for IMS commands. For details, see SEC_CMD* fields. The default class used by IMS for command security is CIMS. Maximum length: 8 characters.

CLASS_DB

This field shows the SAF resource class used for controlling access to databases. The default class used by IMS for database security is PIMS. Maximum length: 8 characters.

CLASS_FIELD

This field shows the SAF resource class used for controlling access to database field names. The default class used by IMS for database field security is FIMS. Maximum length: 8 characters.

CLASS_LTERM

This field shows the SAF resource class used for logical terminals (LTERM). The default class used by IMS for logical terminal security is LIMS. Maximum length: 8 characters.

CLASS_OTH

This field shows the SAF resource class used for controlling access to other resources. The default class used by IMS for other resource security is OIMS. Maximum length: 8 characters.

CLASS_OTMA

This field shows the SAF resource class used for controlling access through Online Transaction Manager Access. The default class used by IMS for OTMA security is RIMS. Maximum length: 8 characters.

CLASS_PSB

This field shows the SAF resource class used for IMS program specification blocks. The default class used by IMS for PSB security is IIMS. Maximum length: 8 characters.

CLASS_SEG

This field shows the SAF resource class used for IMS database segments. The default class used by IMS for database segment security is SIMS. Maximum length: 8 characters.

CLASS_TRAN

This field shows the SAF resource class used for IMS transactions if security is activated for IMS transactions. For details, see the SEC_TRANS_ACTIVE field). The default class used by IMS for transaction security is TIMS. Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

IMS_LEVEL

This field identifies the IMS system release level of the active IMS region.

IMSID

This field identifies the IMS subsystem identification. Maximum length: 8 characters.

JOBID

This field contains the JES job ID of the IMS subsystem. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the IMS subsystem. Maximum length: 8 characters.

RCLASS

This field specifies the resource class suffix. Maximum length: 7 characters.

REGION_TYPE

This field specifies the region type of the IMS subsystem. Field values: Online, DBRC, DL/I, and Batch.

REGION_USERID

This field contains the userid associated with the IMS subsystem. Maximum length: 8 characters.

SEC_AO_CMD

This field specifies how security is handled for automated operator CMD calls. The possible values are:

Allow – Automated operator commands are allowed. No security checking is performed.

Exit – An exit is used to determine if automated operator CMD calls are allowed.

RACF – RACF is used to determine if automated operator CMD calls are allowed.

R/E – RACF and an exit are used to determine if automated operator CMD calls are allowed.

SMU – SMU is used to determine if automated operator CMD calls are allowed.

SEC_AO_ICMD

This field specifies how security is handled for automated operator ICMD calls. The possible values are:

Allow – Automated operator commands are allowed. No security checking is performed.

Deny – No automated operators ICMD calls are allowed.

Exit – An exit is used to determine if automated operator ICMD calls are allowed.

RACF – RACF is used to determine if automated operator ICMD calls are allowed.

R/E – RACF and an exit are used to determine if automated operator ICMD calls are allowed.

SEC_CMD_ALL

This field specifies whether access to commands from static and ETO terminals is checked. Field value: Yes or No.

SEC_CMD_ETO

This field specifies whether access to commands from the ETO terminals is checked. Field value: Yes or No.

SEC_CONSOLE_CMD

This field specifies how console commands are handled. The possible values are:

Allow – Console commands are allowed. No security checking is performed.

Deny – No console commands are allowed.

Exit – An exit is used to determine if console commands are allowed.

RACF – RACF is used to determine if console commands are allowed.

R/E – RACF and an exit are used to determine if console commands are allowed.

SEC_MULTI

This field specifies whether a static user can sign on to multiple static sessions. Field value: Yes or No.

SEC_ODBA

This flag field specifies whether PSBs specified on an APSB call for an ODBA application are protected in the AIMS or A*xxxxxxx* general resource class. Field value: Yes or No.

SEC_PR_CMD_ALL

This field refers to the security settings on the EXEC PARM statement. This field specifies whether access checking is required for commands entered from static and ETO-defined terminals. Field value: Yes or No.

SEC_PR_CMD_ETO

This field refers to the security settings on the EXEC PARM statement. This field specifies whether access checking is required for commands entered from ETO-defined terminals. Field value: Yes or No.

SEC_PR_FUSER

This field refers to the security settings on the EXEC PARM statement and specifies whether user verification is forced. Field value: Yes or No.

SEC_PR_MULTI

This field refers to the security settings on the EXEC PARM statement and specifies whether a static user can sign on to multiple static sessions. Field value: Yes or No.

SEC_PR_PASSWORD_UPPER

This field refers to the security settings on the EXEC PARM statement and specifies whether a password is changed to uppercase when entered. Field value: Yes or No.

SEC_PR_USER

This field refers to the security settings on the EXEC PARM statement and specifies whether user verification is to be performed. Field value: Yes or No.

SEC_RACF_AVAIL

This field specifies that RACF is available for transaction authorization. Field value: Yes or No.

SEC_RASEXIT

This field specifies that resource checking is performed using a resource access security (RAS) exit. Field value: Yes or No.

SEC_RASRACF

This field specifies that resource checking is performed using a RACROUTE call. Field value: Yes or No.

SEC_RE_CMD_ALL

This field refers to the security setting, as entered on the /NRESTART or /ERESTART MTO command or to the console WTOR during IMS system startup, and specifies whether command access is verified for static and ETO-defined terminals. This field is empty if a command security setting is not specified. Field value: Yes or No.

SEC_RE_CMD_ETO

This field refers to the security setting, as entered on the /NRESTART or /ERESTART MTO command or to the console WTOR during IMS system startup, and specifies whether command access is verified for ETO-defined terminals. This field is empty if a command security setting is not specified. Field value: Yes or No.

SEC_RE_MULTI

This field refers to the security setting, as entered on the /NRESTART or /ERESTART MTO command or to the console WTOR during IMS system

startup, and specifies whether a static user can sign on to multiple static sessions. This field is empty if a multiple session setting is not specified. Field value: Yes or No.

SEC_RE_TRANS

This field refers to the security setting, as entered on the /NRESTART or /ERESTART MTO command or to the console WTOR during IMS system startup, and specifies whether transaction authorization is checked. This field is empty if a transaction security setting is not specified. Field value: Yes or No.

SEC_RE_USER

This field refers to the security setting, as entered on the /NRESTART or /ERESTART MTO command or to the console WTOR during IMS system startup, and specifies whether the user verification is to be performed. This field is empty if a user verification setting is not specified. Field value: Yes or No.

SEC_SD_CMD_ALL

This field refers to the security setting as specified during system definition and specifies whether command access is verified for static and ETO-defined terminals. Field value: Yes or No.

SEC_SD_CMD_ETO

This field refers to the security setting as specified during system definition and specifies whether command access is verified for ETO-defined terminals. Field value: Yes or No.

SEC_SD_ENH

This field refers to the security setting as specified during system definition and specifies whether enhanced security has been requested. Field value: Yes or No.

SEC_SD_FTRANS

This field refers to the security setting as specified during system definition and specifies whether transaction authorization is forced. Forcing authorization prevents transaction authorization processing from being overridden and inactivated. Field value: Yes or No.

SEC_SD_FUSER

This field refers to the security setting as specified during system definition and specifies whether user verification is forced. Forcing authorization prevents transaction authorization processing from being overridden and inactivated. Field value: Yes or No.

SEC_SD_MULTI

This field refers to the security setting as specified during system definition and specifies whether a static user can sign on to multiple static sessions. Field value: Yes or No.

SEC_SD_RACFTERM

This field refers to the security setting as specified flag during system definition and specifies whether RACF transaction authorization and sign on processing is required. Field value: Yes or No.

SEC_SD_TRANS

This field refers to the security setting as specified during system definition and specifies whether transaction authorization is performed. Field value: Yes or No.

SEC_SD_USER

This field refers to the security setting as specified during system definition and specifies whether user verification is performed. Field value: Yes or No.

SEC_TCO_RACF

This field specifies whether RACF is used for authorization in time-controlled operation (TCO) requests. Field value: Yes or No.

SEC_TRANS

This field specifies whether transaction authorization checks are performed. Field value: Yes or No.

SEC_TRANS_ACTIVE

This field specifies whether transaction authorization checking is active within the IMS subsystem. Field value: Yes or No.

SEC_USER

This field specifies whether userid verification is performed within the IMS subsystem. Field value: Yes or No.

SEC_USER_ACTIVE

This field specifies whether the userid verification is active within the IMS subsystem. Field value: Yes or No.

SEC_VIOL_LIMIT

This field specifies the maximum number of terminal and password security violations allowed prior to master terminal notification for:

- physical terminals
- transaction commands

STEPNAME

This field contains the step name associated with the IMS subsystem. Maximum length: 8 characters.

SUBSYS_CRC

This field specifies the console command character that is used to enter commands from a console. Length: 1 character.

SVCNO

This field specifies the Type 2 SVC number that is used by the IMS subsystem.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. This field has a maximum length of 8 characters for compatibility with other NEWLIST types.

VTAM_APPLID

This field specifies the specific VTAM application identifier (APPLID) for the IMS subsystem. Maximum length: 8 characters.

IMS_TRANSACTION: IMS transactions

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
				•	•	•

This section documents the fields for the NEWLIST TYPE=IMS_TRANSACTION. This NEWLIST type lists one entry per active IMS transaction for an IMS subsystem in each system. An entry is uniquely identified by the following fields: SYSTEM, COMPLEX, ASID, JOBNAME. and TRANSACTION.

Field descriptions

The IMS_TRANSACTION NEWLIST provides the following fields for reporting.

ASID

This field contains the address space ID associated with the IMS subsystem. The address space ID is a 2-byte hexadecimal number; the JOBNAME field shows the related job.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 353. IMS_TRANSACTION NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CLASS

This field specifies the resource class used to secure the IMS transaction (for example TIMS). Maximum length: 8 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

IMSID

This field specifies the IMS subsystem identification of the IMS subsystem where the IMS transaction is run. Maximum length: 8 characters.

JOBID

This field contains the JES job ID of the IMS subsystem. Maximum length: 8 characters.

JOBNAME

This field contains the JES job name of the IMS subsystem. Maximum length: 8 characters.

PSBNAME

This field specifies the program specification block (PSB) that is associated with the IMS transaction. Maximum length: 8 characters.

QUALIFIED_RESOURCE

This field specifies the qualified resource name. It is the concatenation of the RESOURCE_LOCATION and the RESOURCE separated by a colon, for example: IPO1.IMS.IMS10CR1.TRN:ADDINVNT Maximum length: 30 characters.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and conditional profile name. The default output length is 45 characters, but the profile name can be up to 255 characters so the maximum output length of RACF_ACL is 290 characters.

Use the EXPLODE output modifier for a complete access list including access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use EFFECTIVE to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE. You can use the UNIVERSAL modifier to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_CLASS

This field contains the resource class of the profile that protects the resource. The resource class can be a member class or a grouping class. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 8 characters.

RACF_PROFILE

This field contains the name of the profile that protects the resource. The profile can be a member class profile or a grouping class profile. The RACF_PROFILE and RACF_CLASS fields are part of the repeat group of RACF information. Maximum length: 13 characters.

RACF_UACC

This field contains the effective universal access authority (UACC) to the program. The UACC is determined from all grouping and non-grouping

resource profiles that describe the program. Field values: NONE, READ, EXECUTE, UPDATE, CONTROL, or ALTER.

RESOURCE

This field specifies the resource name used to secure the IMS transaction. Maximum length: 246 characters. Default length: 13 characters.

RESOURCE_LOCATION

This field indicates the environment where the resource is relevant. This field is the concatenation of several fixed strings, fields, and lookups, such as *system*.IMS.*jobname*.PSB. An example is IPO1.IMS.IMS10CR1.PSB. Maximum length: 21 characters.

STEPNAME

This field contains the step name associated with the IMS subsystem. Maximum length: 8 characters.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. Maximum length: 8 characters.

TRAN_CLASS

This field specifies the name of the transaction class for the IMS transaction.

TRANSACTION

This field specifies the name of the IMS transaction. Maximum length: 8 characters.

VTAM_APPLID

This field specifies the VTAM application identifier (APPLID) for this IMS subsystem. Maximum length: 8 characters.

IOAPP: I/O Appendages

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The I/O Appendages (IOAPP) NEWLIST (NEWLIST TYPE=IOAPP) describes authorized I/O appendages. Each entry in this NEWLIST can be uniquely identified by the fields SYSTEM ID or SYSTEM NAME.

Field descriptions

The IOAPP NEWLIST provides the following fields for reporting.

ADDRESS

This field contains the address of the default I/O appendage module, if one resides in-storage. This is the appendage used, unless the user has an appendage in an authorized STEPLIB or in the link list. See also the CONTENT field. The EXIT NEWLIST describes the I/O appendage routine in detail.. See "EXIT: System Exits" on page 1027.

Note: All possible I/O appendages (including those that can only be used with a STEPLIB) are reported by the REPORT AC1.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The following table lists the audit concerns currently defined:

- Non-default Appendage

  An appendage other than IGG019E4. You should review this appendage.
- Altered Default Appendage

  Appendage IGG019E4 with non-default TYPE values. You should review the reason the TYPE values are set to non-default values.
- Added automatically by MVS

  Appendage IGG019E4 with default TYPE values. This appendage is not added automatically.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 354. IOAPP NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

CONTENT, CONTENTS

A string containing up to the first 256 bytes of the appendage, which usually include the eye catcher. The default output length of this string is 128 characters (containing the first 128 bytes of the appendage). In the default output format, the readable text from the contents is shown; the non-printable parts of the contents have been replaced by one or two dots. This is the appendage used, unless the user has an appendage in an authorized STEPLIB. See also the ADDRESS field.

Note: All possible I/O appendages (including those that can only be used with a STEPLIB) are reported by the REPORT AC1.

DEFAULT

This flag field indicates whether the I/O appendage conforms to the (IBM-defined) default. An appendage conforms to the default if both the authorization and the types match. See also the TYPE and DEFAULTTYPE fields.

DEFAULTTYPE

This repeated field indicates the (IBM-defined) default types for which the I/O appendage is authorized. Each appendage belongs to at least one, and at most five, default types. See the TYPE field for a table of values. See also the DEFAULT field.

DESCRIPTION, DESC

This text field contains a description of (the function of) the I/O appendage.

ID

The ID of the authorized I/O appendage. This is a two-character string that completes the required prefix IGG019, for example, ID EA indicates the I/O appendage IGG019EA. See also the NAME field.

NAME

The name of the authorized I/O appendage. This is an eight-character string that contains the full name of the I/O appendage. All names start with the required prefix IGG019. See also the ID field.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types.

TYPE

This repeated field indicates the types for which the I/O appendage is authorized. Each appendage belongs to at least one, and at most five, types. The TYPE values are listed in the following table.

Table 355. TYPE values

I/O appendage types
ABE Abnormal End
CHE Channel End
EOE End of Extent
PCI Program Controlled Interrupt
SIO Start I/O

See also the DEFAULT and DEFAULTTYPE fields.

WHERE

A string indicating the virtual storage area where the appendage resides. This is the appendage used, unless the user has an appendage in an authorized STEPLIB. See also the ADDRESS field.

Note: All possible I/O appendages (including those that can only be used with a STEPLIB) are reported by the REPORT AC1 NEWLIST.

Table 356 on page 1054 lists the possible WHERE values and their meaning. Areas starting with an E reside above 16 MB in virtual storage.

Table 356. IOAPP - WHERE values and descriptions

WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

IP: Profile information for TCP/IP configuration

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

You can use the IP configuration `NEWLIST` statements to select and report on information in the TCP/IP stack configuration. These `NEWLIST`s are supported in zSecure Audit and zSecure Alert.

Each record in the `IP_RESOLVER NEWLIST` is associated with a particular CS Resolver configuration, uniquely identified by the `COMPLEX`, `SYSNAME`, `SYSPLEX`, and `SYSTEM` fields. Each record in the other IP configuration newlists is associated with a particular TCP/IP stack, uniquely identified by the common fields: `COMPLEX`, `STACK`, `SYSNAME`, `SYSPLEX`, and `SYSTEM`. See “Common fields” on page 1055.

In addition to the common fields, each `NEWLIST` has its own fields. The following sections describe IP `NEWLIST` types.

"IP_VIPA: TCP/IP VIPA configuration" on page 1087

In addition to creating these reports using the CARLa NEWLIST command, you can also generate them using the Resources function available on the zSecure Audit menu. See Chapter 4, "Resource reports," on page 383.

You can also process TCP/IP stack configuration information by analyzing SMF data from the TCP/IP profile event record (SMF record type 119, subtype 4) using the SMF reporting functions or the SMF NEWLIST. For details, see Chapter 7, "SMF and HTTP Reporting (Events menu)," on page 545 and the IP* fields documented in "SMF: SMF records" on page 1276.

The TCP/IP stack configuration information is collected by the zSecure Collect program. Collection is enabled and disabled using the TCPIP configuration parameter. For details, see Chapter 16, "zSecure Collect for z/OS," on page 1591.

Common fields

Each record in the IP configuration newlists is associated with a particular TCP/IP stack, uniquely identified by the following fields: COMPLEX, STACK, SYSNAME, SYSPLEX, and SYSTEM fields. These fields are common to all TCP/IP configuration newlists.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The COMPLEX field identifies the security complex that contains the system. The security complex value can come from the ALLOC COMPLEX parameter or can default to the security node or sysplex name.

STACK

The STACK field provides the stack name which is the name of the started task procedure running the stack.

SYSNAME

The SYSNAME field identifies the name of the system. This value is used as part of the SAF resource name in some NEWLIST types.

SYSPLEX

The SYSPLEX field provides the name of the sysplex that the SYSTEM is a part of, if applicable.

SYSTEM

The SYSTEM field is the name of the MVS system, which is equal to the SMF system ID.

For more information about TCP/IP configuration, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

IP_AUTOLOG: TCP/IP autolog configuration

The IP_AUTOLOG NEWLIST selects and reports on autolog configuration data for TCP/IP stacks. The information includes lists of MVS started procedures to be initiated by the Autolog task when TCP/IP stacks are started. You can use the

following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

You can change the values for these fields using AUTOLOG statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_AUTOLOG NEWLIST provides the following fields for reporting.

JOBNAME

Contains the name of the job for the PORT reservation statement. This value can be identical to the value in the PROCNAME field. However, for z/OS UNIX jobs that create listener threads, the value is not the same. If the JOBNAME value is missing, the job name is taken from the PROCNAME field.

OPTIONS

Repeated flag field provides information about the current status of the IP autolog stack configuration options. This field can have the following values:

DELAYSTART DVIPA
The AUTOLOG procedure starts after the TCP/IP stack has joined the sysplex group and has processed its dynamic VIPA configuration.

DELAYSTART TTLS
The AUTOLOG procedure starts after the Policy Agent has successfully installed the AT-TLS policy in the TCP/IP stack and AT-TLS services are available.

PARMSTRING

The parameter string to be added following the START *procedure_name*, where *procedure_name* is the value is found in the PROCNAME field.

PROCNAME

Contains the name of a procedure that the TCP/IP address space must start.

WAIT

If a procedure is still active when TCP/IP is trying to AUTOLOG the procedure during the TCP/IP startup process, this value specifies the number of minutes that TCP/IP waits for the procedure to shut down before attempting to start it again. This situation can occur when a procedure was not shutdown the last time that TCP/IP was shutdown. TCP/IP checks if the procedure has shutdown every ten seconds until the specified time interval expires and restarts the procedure as soon as the procedure has been shutdown. If the shutdown is detected before the time interval expires, the procedure is restarted. If the procedure is still active when the time interval specified by wait expires, then TCP/IP cancels and restarts the procedure.

If WAIT= *0*, TCP/IP does not cancel or restart any active procedures during the initialization process.

IP_INTERFACE: TCP/IP interface configuration

The IP_INTERFACE NEWLIST selects and reports on interface configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as

required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

Field descriptions

The IP_INTERFACE NEWLIST provides the following fields for reporting.

ASSOC_NAME

Provides the associated name for the interface, which can be the name for a Device, OSA-Express port, or a TRLE definition depending on the interface type.

CHPID

Provides the IQD Channel Path Identifier (CHPID) for the HiperSockets interface.

INDEX

Provides the positive number assigned to the interface by the TCP/IP stack when the stack processed the configuration statement for the interface. The index value is used heavily by SNMP as the identifier of an interface for a stack because it is easier to use a number than a name.

INTERFACE

The INTERFACE field contains the name of an IPv4 or IPv6 interface.

INTFID

The INTFID field contains the configured interface ID. This ID is used to form the link-local address for the interface. The value is also appended to any manually configured prefixes for the interface to form complete IPv6 addresses on the interface.

IP

The IP repeat group field provides the IPv4 and IPv6 addresses associated with the interface.

IPMASK

Repeat group field provides the IPv4 subnet masks of the IPv4 addresses associated with the interface. For IPv6 addresses, the IPMASK field is empty, but not missing.

OPTIONS

A repeated flag field that provides information about the settings for the IP stack interface configuration options. Table 357 lists the available configuration options.

Table 357. TCP/IP stack: Interface Configuration - configuration options available

Option	Header
INTERFACE	The INTERFACE statement was employed (as opposed to DEVICE, LINK, or HOME statements).
AUTORESTART	In the event of a device failure, the TCP/IP address space attempts to reactivate the device.
NOAUTORESTART	For most device failures, the TCP/IP address space does not attempt to reactivate this device.
IPBCAST	The link both sends and receives IP broadcast packets.

Table 357. TCP/IP stack: Interface Configuration - configuration options available (continued)

Option	Header
MONSYSPLEX	Sysplex autonomics monitor the status of the link.
NOMONSYSPLEX	Sysplex autonomics do not monitor the status of the link.
DYNVLANREG	If a VLAN ID is configured for this link, it is dynamically registered with the physical switches on the corresponding LAN.
NODYNVLANREG	If a VLAN ID is configured for this link, it must be manually registered with the physical switches on the corresponding LAN.
VMAC ROUTEALL	All IP traffic destined to the virtual MAC is forwarded by the OSA-Express device to the TCP/IP stack. If VMAC_ADDRESS is missing, the OSA-Express feature generates a virtual MAC address.
VMAC ROUTELCL	Only traffic destined to the virtual MAC and whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express. If VMAC_ADDRESS is missing, the OSA-Express feature generates a virtual MAC address.
CHECKSUM	Inbound checksum calculation is performed for all packets received on this interface.
NOCHECKSUM	Inbound checksum calculation is not performed for any packets received on this interface.
ISOLATE	OSA-Express is being prevented from routing packets directly to another TCP/IP stack that share the OSA. In this mode, OSA-Express discards any packets when the next hop address was registered by another stack that share the OSA. Packets can flow between two stacks that share the OSA only by first going through a router on the LAN.
NOISOLATE	Packets are routed directly between TCP/IP stacks sharing the OSA. In this mode, if the next hop address was registered by another stack that share the OSA adapter, then OSA-Express routes the packet directly to the sharing stack without putting the packet on the external LAN.

PFXLEN

A repeat group field that shows the prefix lengths for the subnet address of the IPv4 and IPv6 addresses associated with the interface.

SECCLASS

Provides the security class used for IP filtering with this interface. Valid security classes are integers in the range 1 - 255. The default value is 255.

SOURCEVIPA_INTERFACE

The name of the previously defined static VIPA interface which is used for `SOURCEVIPA`.

TYPE

The TYPE field identifies the Interface type. Table 358 on page 1059 lists the available types.

Table 358. Possible values for the Interface type

Interface type	Description
LOOPBACK6	Loop back interface. One of the IPv6 addresses associated with the interface is ::1. Additional loopback addresses can be defined.
IPAQENET	OSA-Express QDIO Ethernet, OSA-Express2, or OSA-Express3 interface for IPv4
IPAQENET6	OSA-Express QDIO Ethernet or Fast Ethernet interface for IPv6.
IPAQIDIO6	IPv6 HiperSockets interface.
MPCPTP6	MPC Point-To-Point Data Link Control interface. The interface can be used to carry IPv6 traffic over ESCON channels, over XCF links in a sysplex, or between z/OS Communications Server images using the simulated device provided by the IUTSAMEH function in VTAM.
VIRTUAL6 S	Static virtual interface for IPv6. The interface is not associated with real hardware and is used for fault tolerance support.
IPAQIDIO	MPCIPA for HiperSockets - Another TCP/IP within the same CPC.
MPCPTP	MPC Point-To-Point Data Link Control interface. The interface can be used to carry IPv4 traffic over ESCON channels or between z/OS Communications Server images using the simulated device provided by the IUTSAMEH function in VTAM.
VIRTUAL	Static virtual interface for IPv4. The interface is not associated with real hardware and is used for fault tolerance support.
LOOPBACK	Loop back interface. One of the IPv4 addresses associated with the interface is 127.0.0.1. Additional loopback addresses can be defined.

VLAN_ID

Contains the Virtual LAN identifier value. Valid VLAN IDs are in the range 1 - 4094.

VMAC_ADDRESS

The virtual MAC address. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv4 packets sent to and received from this TCP/IP stack. If VMAC_ADDRESS is missing, the OSA-Express device generates a virtual MAC address.

IP_NETACCESS: TCP/IP network access control configuration

The IP_NETACCESS NEWLIST select and report on the network access control configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

The field values reported in the IP_NETACCESS NEWLIST can be changed through the use of NETACCESS statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_NETACCESS NEWLIST provides the following fields for reporting.

INBOUND

The INBOUND flag field indicates whether network access control checking is enabled for inbound socket commands.

IP

Specifies an IP address or value that identifies the network or networks that require security product access control for user requests. This field can have the following values:

IP address
Security product access control of user requests is required for the network with the specified IP address.

DEFAULT
Security product access control of user requests is required for any networks not specifically defined by other NETACCESS statement entries.

DEFAULTHOME
Security product access control of user requests is required for all IP addresses that are local to this stack and not specifically defined by other NETACCESS statement entries.

IPMASK

Contains the IPv4 subnet mask. If the destination address is in IPV6 format, this field is missing.

OUTBOUND

Flag field that indicates whether network access control checking is enabled for outbound socket commands.

PFXLEN

The PFXLEN field contains the prefix length of the Subnet address.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE, so it works best if specified in the scope of a NEWLIST, while there are no outer selections or with the UNIVERSAL modifier specified to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See “Format names for input and output” on page 810.

RACF_PROFILE

Identifies the profile which protects the resource identified in the IP_RESOURCE field. The profile is simulated with the current RACF database.

RESNAME

Contains the last qualifier of the resource name found in the RESOURCE field. Effective user IDs permitted to this resource are allowed to access the network.

RESOURCE

Identifies an SAF SERVAUTH resource. Effective user IDs with permissions for this resource can access the network. The resource name has the following format: EZB..*sysname.tcpname.resname* where the variable identifiers have the following meanings:

sysname is the value of the MVS &SYSNAME. system symbol. The value comes from the SYSNAME field.

tcpname is the name of the procedure used to start the TCP/IP stack. The value comes from the STACK field.

resname is the 8-character value following the network specification in a statement. The value comes from the RESNAME field.

IP_PORT: TCP/IP port configuration

The IP_PORT NEWLIST selects and reports on port configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

The field values for the IP_PORT NEWLIST fields can be changed with PORT and PORTRANGE statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_PORT NEWLIST provides the following fields for reporting.

AUDITCONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs. The contents is subject to change.

This field can contain one or more concerns separated by commas. The following audit concerns have been defined:

Because there is no SAF parameter, any user or program can bind to a privileged [TCP|UDP] port [*begin_port-end_port*|*port***] under jobname** *jobname* **(filter) by default, thus masquerading as a legitimate service and receive passwords**

The TCP/IP stack configuration contains a PORT or PORTRANGE statement pertaining to TCP or UDP ports *begin_port* to *end_port*, or to port *port*. The statement has a parameter jobname which specifies the MVS job names that can use the specified ports. Because the statement has no SAF parameter, no RACF resource is checked to verify that a user or program is permitted to bind to the ports. Unless a PORT statement with a more specific jobname filter has been specified to prohibit access, any user or program can bind to the ports using a job name that matches the name specified in the PORT or PORTRANGE statement. Thus, the user or program can masquerade as a legitimate service. The compromised service can then be used to steal passwords because the port, or at least one of the ports in range, is associated with the transmission of a clear text password.

Because there is no SAF parameter, any user or program can bind to a privileged [TCP|UDP] port [*begin_port-end_port*|*port*] under jobname *jobname* (filter) by default, thus masquerading as a legitimate service

The TCP/IP stack configuration contains a PORT or PORTRANGE statement pertaining to TCP or UDP ports *begin_port* to *end_port*, or to port *port*. The statement has a *jobname* parameter which specifies the MVS job name that can use the specified ports. no RACF resource is checked to verify that a user or program is permitted to bind to the ports. Unless a PORT statement with a more specific jobname filter has been specified to prohibit access, any user or program can bind to the ports using a job name that matches the name specified in the PORT or PORTRANGE statement. Thus, the user or program can masquerade as a legitimate service.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 359. IP_PORT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

BEGIN_PORT

Contains the first port in a range of reserved ports. If ports have not been reserved (UNRSV=true), this field is missing. You can change this field value with PORT and PORTRANGE statements.

BIND

Contains the IP address *ipaddr* which is associated with the job name present in the JOBNAME field. When a job with the designated name binds to the IPv4 INADDR_ANY address, or to the IPv6 address in6addr_any, the bind is intercepted and converted to a bind to the IP address specified by *ipaddr*. Subsequent bind processing occurs as though the server instance had originally issued the bind to the IP address *ipaddr*. You can change this field value with PORT statements.

COUNT

Contains the number of ports in a range of reserved ports. If the ports are not reserved (UNRSV= true), this field is missing. The field value can change through the use of PORT and PORTRANGE statements.

END_PORT

Contains the last port in a range of reserved ports. If the ports are not reserved (UNRSV= true), this field is missing. You can change this field value with PORT and PORTRANGE statements.

JOBNAME

Specifies an MVS job name filter. If the value of the USE field is *JOBNAME*, then the JOBNAME field indicates which job names can use the ports in the BEGIN_PORT to END_PORT range, or any unreserved port in case the value of UNRSV is true. For

multiple TCP reservations for the same port or for multiple PORT UNRSV statements for the same protocol, the TCP/IP stack searches the PORT statements for the closest match (if any) to the application job name. The field value can change through the use of PORT and PORTRANGE statements.

OPTIONS

The OPTIONS repeated flag field provides information about the current status of IP interface settings. Table 360 lists the settings that are reported.

Table 360. TCP/IP Configuration IP_PORT - Interface settings reported

OPTION	Description
NOAUTOLOG	The TCP/IP address space is not to restart the server if it was stopped previously.
DELAYACKS	Transmission of acknowledgments is delayed when a packet is received with the PUSH bit on in the TCP header. By default, this setting only affects connections that use a port in the specified port range. The behavior can be overridden by specifying the NODELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection: • The TCP/IP stack BEGINROUTES or GATEWAY profile statements • The Policy Agent RouteTable statement • The OMPROUTE configuration statements
NODELAYACKS	An acknowledgment is returned immediately when a packet is received with the PUSH bit on in the TCP header. Only connections that use this port are affected. Specifying the NODELAYACKS parameter on the PORTRANGE statement overrides the specification of the parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection: • The TCP/IP stack BEGINROUTES or GATEWAY profile statements • The Policy Agent RouteTable statement • The OMPROUTE configuration statements
SHAREPORT	TCP/IP allows multiple listeners to listen on the same combination of port and interface. Incoming connection requests for a port are distributed among the listeners using a weighted round-robin distribution method based on the accept Efficiency Fractions (SEFs) of the listeners sharing the port.
SHAREPORTWLM	TCP/IP allows multiple listeners to listen on the same combination of port and interface. The listener selection is based on WLM server-specific recommendations, modified by the SEF values for each listener.
DENY	Access to unreserved ports is denied. The JOBNAME is an asterisk (*) in this case.
WHENLISTEN	Port access control is targeted to TCP applications acting as servers[10] that issue an explicit bind to a user-specified unreserved port. Permission to use the unreserved port is determined when a TCP listen command is issued. If a listen command is not issued, no access control check is made.

Table 360. TCP/IP Configuration IP_PORT - Interface settings reported (continued)

OPTION	Description
WHENBIND	Permission to use an unreserved port is determined when an explicit bind to a specific local port is issued. For the UDP protocol, it can affect UDP applications that bind to a specific local port. For the TCP protocol, it can affect TCP client applications that bind to a specific local port for outbound connections.

PORTRANGE

Indicates whether a PORTRANGE statement was used instead of a PORT statement. The field value can change through the use of PORT and PORTRANGE statements.

PROTOCOL

The PROTOCOL field specifies the protocol associated with a range of ports. The value can be TCP or UDP. You can use the PORT and PORTRANGE statements to change the value of this field.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE, so it works best if specified in the scope of a NEWLIST, while there are no outer selections or with the UNIVERSAL modifier specified to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_PROFILE

Identifies the profile which protects the RESOURCE *resource*. The profile is simulated with the current RACF database. You can use the PORT and PORTRANGE statements to change the value of this field.

RESNAME

Contains the last qualifier of the SAF SERVAUTH resource name present in the RESOURCE field. All ports in the BEGIN_PORT to END_PORT port range (or all unreserved ports in case UNRSV is true) are reserved for users that are permitted to this resource. You can use the PORT and PORTRANGE statements to change the value of this field.

RESOURCE

10. Applications acting as servers are able to accept incoming client TCP connections.

The name of a SAF SERVAUTH resource. All ports in the BEGIN_PORT to END_PORT port range (or all unreserved ports in case UNRSV is true) are reserved for users that are permitted to this resource.

You can use the PORT and PORTRANGE statements to change the value of this field.

The following code shows a sample resource.

```
EZB.PORTACCESS.sysname.tcpname.resname
```

where the variable identifiers have the following meanings:

- *sysname* is the value of the MVS &SYSNAME. system symbol, which is present in the SYSNAME field.
- *tcpname* is the name of the procedure used to start the TCP/IP stack. This value is also found in the STACK field
- *resname* is the 8-character value following the SAF keyword in a PORT or PORTRANGE statement. This value is also found in the RESNAME field.

UNRSV

The UNRSV flag field indicates whether a PORT UNRSV statement was used. Such statements indicate which applications or users are permitted to access application-specified unreserved ports. The following processing rules apply to PORT UNRSV statements:

- PORT UNRSV statements control access to all unreserved ports in the range 1 - 65535 unless RESTRICTLOWPORTS is configured. However, when RESTRICTLOWPORTS is configured, PORT UNRSV statements control access to unreserved ports above port 1023 only.
- For UDP, access control is applied when an application issues a bind to a particular port number to establish a local port. For TCP, access control is applied depending on the value of the WHENBIND or WHENLISTEN parameter.
- If neither DENY nor the SAF keyword is specified, an application that matches the protocol and specified job name on a PORT UNRSV statement can access unreserved ports. The job name can be an asterisk (*). If *DENY* is specified, all applications are denied access to unreserved ports for the specified protocol.
- If the SAF keyword is specified, applications that match the PORT UNRSV statement must also have user access to the SAF SERVAUTH resource to be permitted to access an unreserved port.

You can use PORT statements to change the value of this field.

USE

The USE field indicates how the port is used. Table 361 lists the possible use types. You can change this field value by using PORT and PORTRANGE statements.

Table 361. TCP/IP Configuration IP_PORT: Port use types

Port use type	Meaning
RESERVED	Specifies that the ports in the BEGIN_PORT to END_PORT range are not available for use by any user. If UNRSV=*true*, none of the unreserved ports are available.
AUTHPORT	Specifies that the ports in the BEGIN_PORT to END_PORT range are not available for use by any user except FTP. FTP can only use the ports if it has been configured to support the PASSIVEDATAPORTS option.
JOBNAME	The JOBNAME field contains a filter indicating which job names can use the ports in the BEGIN_PORT to END_PORT range (or unreserved ports in case UNRSV is true).

IP_RESOLVER: CS Resolver configuration

The IP_RESOLVER NEWLIST describes Communications Server (CS) Resolver configuration settings. The CS Resolver acts on behalf of programs as a client to:

- access name servers for providing name-to-address or address-to-name resolution
- allocate and read the TCPIP.DATA file
- establish TCP/IP stack affinity for certain socket APIs
- provide protocol and services information

Each record in an IP_RESOLVER NEWLIST is associated with a particular CS Resolver configuration, which is uniquely identified by the IP_RESOLVER NEWLIST key comprised of the common fields: COMPLEX, SYSNAME, SYSPLEX, and SYSTEM. See "Common fields" on page 1055.

Field descriptions

The IP_RESOLVER NEWLIST provides the following fields for reporting.

ALWAYSWTO

A flag field that indicates whether some TCP/IP servers, such as SMTP, SNMPQE, LPD, and miscellaneous server, issue all of their messages to the operator console as Write To Operator (WTO) messages in addition to sending messages to the server's MVS job log output. Because of the large volume of operator console messages that can result if ALWAYSWTO is set to YES, ALWAYSWTO is set to NO by default. With the default setting of NO, TCP/IP server messages are not issued as WTO messages.

For this field to be nonempty in report output, the ALWAYSWTO statement must be specified in the global TCPIP.DATA file.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The audit concerns include the following:

- Any user can redirect all DNS queries from the user's address space

  Any user can control which resolver statements are used for name resolution because there is no resolver setup file with a GLOBALTCPIPDATA statement

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 362. IP_RESOLVER NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

AUTOQUIESCE
A flag field indicating whether the resolver will stop sending DNS queries to unresponsive name servers. In the resolver setup file, specify this field as a parameter of the UNRESPONSIVETHRESHOLD statement.

CACHE

A flag field that indicates whether caching is enabled for resolved DNS queries. System-wide caching is enabled by default. To explicitly enable system-wide caching, use the CACHE statement in the resolver setup file. To disable system-wide caching, use the NOCACHE statement in the resolver setup file; caching can also be disabled by specifying the NOCACHE statement in a TCPIP.DATA file.

CACHESIZE

A field that indicates the amount of storage that the resolver can allocate to manage cached records. The storage amount is specified by using the CACHESIZE statement in the resolver setup file. If the NOCACHE statement is specified, the CACHESIZE storage amount is ignored. The default cache size is 200 MB, where 1 MB represents 1048576 bytes.

COMMONSEARCH

A flag field indicating that the resolver uses a common search order for local host files for IPv4 and IPv6 name queries. By default, a different search order is used for IPv4 and IPv6 name queries. In the resolver setup file, use the COMMONSEARCH statement to specify a common search order, and use NOCOMMONSEARCH to specify a different search order.

DATASETPREFIX

A field that identifies the high-level qualifiers for dynamically allocated TCP/IP data sets. The default high-level qualifier is TCPIP. To specify different high-level qualifiers, use the DATASETPREFIX statement in a TCPIP.DATA file.

DBCS_TABLE_NAME

This field is an alias of the LOADDBCSTABLES field.

DEFAULTIPNODES

This field contains the fully-qualified z/OS UNIX file name or MVS data set name of the default IPNODES local host file. Local host files map host names to hard-coded IP addresses. The value of the DEFAULTIPNODES field signifies the final location where the local host file is searched.

In the resolver setup file, the DEFAULTIPNODES statement specifies the fully-qualified name of the default IPNODES local host file.

DEFAULTTCPIPDATA

This field identifies a fully-qualified z/OS UNIX file name or MVS data set name that is the last file searched by the resolver for TCPIP.DATA statements. This value is specified by the DEFAULTTCPIPDATA statement in the resolver setup file. If a DEFAULTTCPIPDATA statement is not specified in the resolver setup file, the default TCPIP.TCPIP.DATA file is searched.

DOMAIN

This field is an alias of the DOMAINORIGIN field.

DOMAINORIGIN, DOMAIN, SEARCH

A repeated field. Each entry is a domain origin that is appended to a host name to form the fully-qualified domain name of the host. A domain origin is appended, in the order listed, until an IP address is found or the list is exhausted. The domain origins are appended for name server queries and for local host table searches. A single domain origin can be specified by the DOMAINORIGIN and DOMAIN statements in a TCPIP.DATA file. Multiple domain origins can be specified by one or more SEARCH statements in a TCPIP.DATA file.

For this field to be nonempty in report output, the DOMAINORIGIN, DOMAIN, or SEARCH statement must be specified in the global TCPIP.DATA file.

GLOBALIPNODES

This field contains the fully-qualified z/OS UNIX file name or MVS data set name of the global IPNODES local host file. Local host files map host names to hard-coded IP addresses. The value of the GLOBALIPNODES field signifies the first location where the local host file is searched.

In the resolver setup file, the GLOBALIPNODES statement specifies the fully-qualified name of the global IPNODES local host file.

GLOBALTCPIPDATA

This field identifies the fully-qualified z/OS UNIX file name or MVS data set name that contains global TCPIP.DATA statements for the entire MVS image and for all TCP/IP data stacks. This value is specified by the GLOBALTCPIPDATA statement in the resolver setup file. It is the first file that the resolver searches for TCPIP.DATA statements.

GLOBALTCPIPDATA_SPEC

A flag field that indicates whether the resolver setup file contains the GLOBALTCPIPDATA statement. If the resolver setup file does not contain a GLOBALTCPIPDATA statement, or if the CS Resolver is not using a resolver setup file, the value of the GLOBALTCPIPDATA_SPEC field is No.

HOSTNAME

This field identifies the TCP host name of the z/OS CS server. The HOSTNAME statement in a TCPIP.DATA file specifies the TCP host name.

For this field to be nonempty in report output, the HOSTNAME statement must be included in the global TCPIP.DATA file.

LOADDBCSTABLES, DBCS_TABLE_NAME

A repeated field. Each field entry is the name of a DBCS translation table to be loaded by the FTP server and client. The LOADDBCSTABLES statement in a TCPIP.DATA file is used to specify DBCS translation tables.

For this field to be nonempty in report output, the LOADDBCSTABLES statement must be included in the global TCPIP.DATA file.

LOOKUP

This field specifies the order in which the DNS and local host file are to be used for name resolution. The LOOKUP field can have one of the following values: DNS, DNS LOCAL, LOCAL, LOCAL DNS.

For this field to be nonempty in report output, the LOOKUP statement must be included in the global TCPIP.DATA file.

DNS

For this value, only the domain name servers specified by the NSINTERADDR and NAMESERVER statements are used for name resolution. When system-wide

caching is enabled, the resolver first queries the resolver cache for entries provided by these name servers on previous name resolution attempts; if that query fails, the resolver then queries the domain name servers to resolve the resource name.

This value is specified in a TCPIP.DATA file by using the LOOKUP statement: LOOKUP DNS.

DNS LOCAL
For this value, the resolver first uses the resolver cache, if caching is enabled, for name resolution. If the resource name is not resolved, the resolver queries name servers directly. If the resource name is still not resolved, the resolver finally queries local host tables to resolve the resource name. DNS LOCAL signifies the default order in which the DNS and local host file are to be used for name resolution.

This value can be explicitly specified in a TCPIP.DATA file by using the LOOKUP statement: LOOKUP DNS LOCAL.

LOCAL
For this value, the resolver only uses the local host tables (for example, /etc/hosts, HOSTS.SITEINFO, or HOSTS.ADDRINFO) for name resolution.

This value is specified in a TCPIP.DATA file by using the LOOKUP statement: LOOKUP LOCAL.

LOCAL DNS
For this value, the resolver first uses local host tables for name resolution. If the resource name is not resolved, the resolver then queries the resolver cache, if caching is enabled. If there is still no resolution, then this is followed by direct queries to the name servers to resolve the resource name.

This value is specified in a TCPIP.DATA file by using the LOOKUP statement: LOOKUP LOCAL DNS.

MAXTTL

This field value specifies the maximum amount of time, in seconds, that the resolver is permitted to use the cached resource information obtained from a Domain Name System (DNS) server. The time-to-live value default is 2147483647 seconds.

In the resolver setup file, a MAXTTL statement can be employed to specify the time-to-live value.

NAMESERVER

This field is an alias of the NSINTERADDR field.

NSPORTADDR

This field identifies the name server port number. The port number pertains to all IP addresses in the NSINTERADDR field. The default port number is 53.

For this field to be nonempty in report output, the NSPORTADDR statement must be included in the global TCPIP.DATA file.

NSINTERADDR, NAMESERVER

A repeated field. Each entry is the IP address of a name server. The port number of the NSPORTADDR field pertains to all of these IP addresses.

For this field to be nonempty in report output, a NSINTERADDR or NAMESERVER statement must be specified in the global TCPIP.DATA file.

OPTIONS_NDOTS

A field of value *n* indicates that for domain names containing *n* periods or more, the resolver should look up the name *as is* before applying the DOMAINORIGIN or SEARCH statement settings. The default value is 1 period.

For this field to be nonempty in report output, the OPTIONS NDOTS statement must be specified in the global TCPIP.DATA file.

PREFERRED_ADDRESS

A repeat group field. PREFERRED_ADDRESS field values combined with up to 4 PREFERRED MASK field values (1 to 24) make up an ordered list of network numbers (subnets or networks) for the resolver to prefer if multiple addresses are returned as the result of a name query.

The ordered list sorts:

- addresses returned by gethostbyname calls
- IPv4 addresses returned for getaddrinfo calls

For this field to be nonempty in report output, the SORTLIST statement must be specified in the global TCPIP.DATA file.

PREFERRED_MASK

A repeat group field. Up to 4 PREFERRED_MASK field values (1 to 24) are combined with PREFERRED_ADDRESS field values to make up an ordered list of network numbers (subnets or networks) for the resolver to prefer if multiple addresses are returned as the result of a name query.

The ordered list sorts:

- addresses returned by gethostbyname calls
- IPv4 addresses returned for getaddrinfo calls

For this field to be nonempty in report output, the SORTLIST statement must be specified in the global TCPIP.DATA file.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE, so it works best if specified in the scope of a NEWLIST, while there are no outer selections or with the UNIVERSAL modifier specified to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RESOLVERTIMEOUT

A field that specifies number of milliseconds that the resolver waits for a response from a name server when using the UDP communication protocol. The default timeout is 5000 milliseconds (5 seconds).

For this field to be nonempty in report output, the RESOLVERTIMEOUT statement must be specified the global TCPIP.DATA file.

RESOLVERUDPRETRIES

A field that specifies how many times (including retries) the resolver attempts to connect to the name server when using UDP datagrams. The default number of connection attempts is 1.

For this field to be nonempty in report output, the RESOLVERUDPRETRIES statement must be specified in the global TCPIP.DATA file.

RESOLVEVIA_TCP

A flag field that indicates whether the resolver uses the TCP protocol to communicate with the name server. The default communication protocol is UDP.

To specify usage of the TCP protocol, in a TCPIP.DATA file, use the statement RESOLVEVIA_TCP.

To explicitly specify usage of the UDP protocol, in a TCPIP.DATA file, use the statement RESOLVEVIA_UDP.

For this field to be nonempty in report output, the RESOLVEVIA statement must be specified in the global TCPIP.DATA file.

SEARCH

This field is an alias of the DOMAINORIGIN field.

SETUP_FILE

A field that lists the name of the resolver setup file, either an MVS data set name or a z/OS UNIX file name. This file contains resolver configuration statements.

If the CS Resolver does not use a resolver setup file, this field is empty in the report output.

SETUP_FILE_EMPLOYED

A flag field indicating whether the CS Resolver employs a resolver setup file.

SOCKTESTSTOR

A flag field that indicates whether TCP/IP C socket calls are being checked for storage access errors on the parameters to the call; by default, C socket calls are not checked for storage access errors.

To enable checking, specify the SOCKTESTSTOR statement in a TCPIP.DATA file.

To explicitly disable checking, specify SOCKNOTESTSTOR statement in a TCPIP.DATA file.

For this field to be nonempty in report output, a SOCKTESTSTOR or SOCKNOTESTSTOR statement must be specified in the global TCPIP.DATA file.

TCPIPJOBNAME, TCPIPUSERID

This field lists the member name of the procedure used to start the TCP/IP address space. The member name can be specified by the TCPIPJOBNAME or TCPIPUSERID statements in a TCPIP.DATA file. The TCPIPJOBNAME field should show as blanks for systems with multiple TCP/IP stacks.

For this field to be nonempty in report output, the TCPIPJOBNAME statement must be included in the global TCPIP.DATA file.

TCPIPUSERID

This field is an alias of the TCPIPJOBNAME field.

UNRESPONSIVETHRESHOLD

This field lists the threshold value that determines when the resolver declares a DNS name server to be unresponsive. The value is a percentage of the resolver queries occurring within a 5-minute sliding interval. If percentage of query failures to a name server is greater than or equal to the threshold percentage value, the resolver considers the name server to be unresponsive.

In the response setup file, the threshold value is specified by the UNRESPONSIVETHRESHOLD statement. If the AUTOQUIESCE parameter of the UNRESPONSIVETHRESHOLD statement is not specified, the default threshold is 25 percent. See "AUTOQUIESCE" on page 1067.

IP_ROUTE: TCP/IP route configuration

The IP_ROUTE NEWLIST selects and reports on route configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

The field values for the IP_ROUTE NEWLIST fields can be changed with BEGINROUTES statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_ROUTE NEWLIST provides the following fields for reporting.

DSTIP

Specifies the destination IPv4 or IPv6 address. A DEFAULT keyword in this field specifies a default IPv4 route. A DEFAULT6 keyword in this field specifies a default IPv6 route. The field value can be changed through the use of BEGINROUTES statements.

INTERFACE

The name of the interface through which packets are sent to the destination. When the interface configuration statement is processed, this name value is indexed by the INTERFACE_INDEX field so the interface can be identified by a numeric value instead of a name.

INTERFACE_INDEX

A positive number assigned to the interface by the TCP/IP stack when the interface configuration statement was processed. In the SNMP protocol, this value is generally used to identify the interface for a stack because it is easier to use a number than a name.

IPMASK

Provides a BSD style address mask of an IPv4 destination address. For IPv6 addresses, the IPMASK field is empty, but not missing.

NEXTHOP_IP

Specifies the host IPv4 or IPv6 address of a gateway or router that you can reach directly, and that forwards packets for the destination network or host.

PFXLEN

The number of mask bits of an IPv4 destination address or the prefix length of an IPv6 destination address.

REPLACEABLE

Flag field that indicates that the static route can be replaced by OMPROUTE and router advertisements when a dynamic route to the same destination is discovered.

REPLACED

Flag field that indicates that the route is a replaceable static route that has been replaced by a dynamic route. The route is not currently being used by the TCP/IP stack.

IP_RULE: TCP/IP Rule Configuration

The IP_RULE NEWLIST selects and reports on the IP filter rule configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

The field values within an IP_RULE NEWLIST can be changed through the use of IPSEC statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_RULE NEWLIST provides the following fields for reporting.

CODE

Specifies the Internet Control Message Protocol (ICMP) code for IP traffic. This field is only applicable when the PROTOCOL is ICMP and the TYPE field has a value other than asterisk (*). For IP traffic to be permitted by this rule, the ICMP code of the traffic must match the value in the CODE field. If the value of CODE is asterisk (*), any ICMP code matches. Also see the TYPE field.

DSTIP

Provides the destination IP address for the outbound rule. For outbound IP traffic to be permitted by this rule, the destination IP address of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the source IP address of the traffic must match this parameter.

DSTIPMASK

The DSTIPMASK field provides the destination IPv4 subnet mask. If the destination address is IPv6, this field is missing.

DSTPFXLEN

The DSTPFXLEN field provides the destination subnet address prefix length.

DSTPORT

For TCP or UDP traffic, the DSTPORT field specifies the destination port for the outbound rule and the source port for the generated inbound rule. Outbound

traffic is permitted if the destination port matches the DSTPORT value. Inbound traffic is permitted if the source port matches the DSTPORT value.

LOG

Flag field that indicates whether packet filter logging is enabled for the default filter rule.

PROTOCOL

Indicates the type of traffic that the rule applies to. For example, rules that permit or prevent IP traffic have the value `PROTOCOL=TCP`. The value can be any of the following protocol types: *ICMP*, *TCP*, *UDP*, *ICMPV6*, *OSPF*, and *nn* for traffic identified by protocol number `nn`.

ROUTING

The ROUTING field indicates the type of packet routing that this rule applies to.

Table 363. IP_RULE ROUTING field - possible values

Routing value	Meaning
LOCAL	Indicates that this rule applies to packets destined for this stack.
ROUTED	Indicates that this rule applies to packets being forwarded by this stack.
EITHER	Indicates that this rule applies to forwarded and non-forwarded packets.

SECCLASS

The SECCLASS field shows the Security class. The value can be an integer in the range 0 – 255 and has a default value of 0. A value of 0 matches any security class value coded on the corresponding profile statement which defines the interface.

SRCIP

The SRCIP field provides the source IP address for the outbound rule. For outbound IP traffic to be permitted by this rule, the source IP address of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the destination IP address of the traffic must match this parameter.

SRCIPMASK

The SRCIPMASK field provides the destination IPv4 subnet mask. If the source address is IPv6, this field is missing.

SRCPFXLEN

The SCRCPFXLEN field provides the prefix length for the source subnet address.

SRCPORT

For TCP or UDP traffic, the SRCPORT field specifies the source port for the outbound rule. For outbound IP traffic to be permitted by this rule, the source port of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the destination port of the traffic must match this parameter.

TYPE

The TYPE field specifies a value for the Internet Control Message Protocol (ICMP) type. Valid values are an asterisk (*) or in the range 0-255, The default is asterisk (*). This value is only applicable when the PROTOCOL is ICMP. For IP traffic to be permitted by this rule, the ICMP type of the traffic must match this parameter value. If TYPE=*, any ICMP type matches. Also see the CODE field.

IP_STACK: TCP/IP stack configuration

The IP_STACK NEWLIST selects and reports on TCP/IP stack configuration. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

Most of the IP_STACK NEWLIST fields provide information that can be changed with the following commands: IPCONFIG, IPCONFIG6, GLOBALCONFIG, IPSEC, SMFCONFIG, SACONFIG, NETMONITOR, UDPCONFIG, and TCPCONFIG statements.

Field descriptions

The IP_STACK NEWLIST provides the following fields for reporting.

AUDITCONCERN
Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs. The contents is subject to change.

The following audit concerns can be returned.

Ports below 1024 are not reserved - any user or program can bind to low [TCP|UDP] ports to masquerade as a legitimate service
TCP or UDP ports 1-1023 are no longer reserved for users by the PORT and PORTRANGE statements. As a result, any user or program can bind to low TCP or UDP ports, thus masquerading as a legitimate service.

IPv[4|6] IP filtering support and IPSec tunnel support not active
IPv4 or IPv6 IP filtering support and IPSec tunnel support are not active.

No audit trail of attacks stopped by filter rules
Logging is not enabled for packet filtering.

No audit trail of attacks stopped by default filter rules
Logging is not enabled for packets that are denied by the implicit default rules.

SMF119 *NN* **is not written - audit trail incomplete**
SMF 119 records are not written when any of the following events occur.

- A user initiates the FTP client command (FTPCLIENT).
- Statistics related to LINK utilization become available (IFSTAT).
- A tunnel is added, removed, activated, or deactivated (IPSECURITY).
- Statistics related to reserved PORT utilization become available (PORTSTAT).
- A TCP connection is established (TCPINIT).
- ATCP/IP stack is activated or terminated (TCPIPSTACK).
- TCP/IP statistics become available (TCPIPSTAT).
- A TCP connection is terminated (TCPTERM).
- The TSO Telnet Client code starts or ends a connection (TN3270CLIENT).
- A UDP socket is closed (UDPTERM).

No access control to/from foreign and local networks
Network access control has not been configured.

No access control required to/from foreign networks
Security product access control of user requests is not required for any network not specifically defined by other (non-DEFAULT) NETACCESS statement entries in the TCP/IP stack configuration.

No access control in local network
Security product access control of user requests is not required for any IP address that is local to this stack and that is not specifically defined by other (non-DEFAULTHOME) NETACCESS statement entries in the TCP/IP stack configuration.

By default, anyone can modify TCP/IP security parameters
By default, all users are permitted to issue VARY TCPIP,,OBEYFILE operator commands. This concern can be caused by any of the following conditions:

- The OPERCMDS class is inactive.
- The OPERCMDS resource MVS.VARY.TCPIP.OBEYFILE is not covered by a profile.
- The resource is covered by a profile with UACC or ID(*) (default) access of CONTROL or higher.

Denial-of-service possible without authentication

By default, all users are permitted to issue VARY TCPIP,,DROP, VARY TCPIP,,STRTSTOP, or VARY TCPIP,,SYSPLEX operator commands. This concern can be issued due to any of the following conditions:

- The OPERCMDS class is inactive.
- Any of the following OPERCMDS resources is not covered by a profile: MVS.VARY.TCPIP.DROP, MVS.VARY.TCPIP.STRTSTOP, or MVS.VARY.TCPIP.SYSPLEX.
- Any of the following resources is covered by a profile with UACC or ID(*) (default) access of CONTROL or higher: : MVS.VARY.TCPIP.DROP, MVS.VARY.TCPIP.STRTSTOP, or MVS.VARY.TCPIP.SYSPLEX.

By default, anyone can read netstat [*netstatoption*] output that might help attackers

By default, all users are permitted to read the output of netstat netstatoption commands. They can use this output to obtain network information that can be exploited to mount an attack. The netstatoption value can be any of the following option values: *ALL*, *ALLCONN*, *ARP*, *BYTEINFO*, *CACHINFO*, *CLIENTS*, *CONFIG*, *CONN*, *DEFADDRT*, *DEVLINKS*, *GATE*, *HOME*, *IDS*, *ND*, *PORTLIST*, *RESCACHE*, *ROUTE*, *SLAP*, *SOCKETS*, *SRCIP*, *STATS*, *TELNET*, *TTLS*, *UP*, *VCRT*, *VDPT*, *VIPADCFG*, or *VIPADYN*. If by default, all users are permitted to read the output of all netstat commands, the netstatoption value in the audit concern message is omitted.This concern can be issued due to any of the following conditions:

- The SERVAUTH class is inactive.
- SERVAUTH resource EZB.NETSTAT.systemname.tcpipstackname.netstatoption is not covered by a profile.
- The resource is covered by a profile with UACC or default ID(*) (default) access of *READ* or higher.

The audit concerns are listed in the following table. The audit priorities can be found in 6.2.2.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 364. IP_STACK NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

DATETIME_STARTED

The DATETIME_STARTED field provides the date and time that the TCP/IP stack was started. The format of this field is DATETIME.

DSNMEM

A repeated field that contains a profile information entry for each data set name followed by a member name between brackets [membername] member between brackets). The data set name entries can originate from the following sources: an `OBEYFILE` command, the default library found in the standard search sequence, or an `INCLUDE` statement.

DYNAMICXCF_INTFID

Specifies the interface ID which is used to form the link-local address for the interface. If this field is missing, TCP/IP generates a random value to be used to form the link-local address. The field value can be changed through the use of `IPCONFIG6` statements.

DYNAMICXCF_IP

Contains the IP address to be used as the home address for all dynamically generated XCF, Same Host, and HiperSockets links. The field value can be changed through the use of `IPCONFIG` statements.

DYNAMICXCF_IPMASK

Specifies the interface-level subnet mask for the `DYNAMICXCF` link. If using `OMPROUTE`, this value is overridden with a corresponding `OMPROUTE` interface parameter value that can be coded or set to the default value. The field value can be changed through the use of `IPCONFIG` statements. If the destination address is IPv6, the `DYNAMICXCF_IPMASK` field is missing.

DYNAMICXCF_IP6

Specifies the fully qualified IPv6 address that is used for all dynamically generated XCF, Same Host, and HiperSockets interfaces. The field value can be changed through the use of `IPCONFIG6` statements.

DYNAMICXCF_PFXLEN

Specifies the number of leftmost significant bits for the address mask. The field value can be changed through the use of `IPCONFIG` statements.

DYNAMICXCF_PFXLEN6

Specifies the length of the routing prefix. If this field is not missing and if `DYNAMICXCF` generates a HiperSockets interface definition, TCP/IP creates a

prefix route over the HiperSockets interface using the number of bits specified in DYNAMICXCF_PFXLEN6 field of the DYNAMICXCF_ADDRESS6 field. Therefore, you can configure other stacks outside the sysplex for the same IQD CHPID using IP addresses with the same prefix. This configuration automatically provides this stack with a route to the other stacks over the HiperSockets interface generated by DYNAMICXCF. If DYNAMICXCF_PFXLEN6 is missing, then TCP/IP does not create a prefix route over the HiperSockets interface. For interfaces other than HiperSockets which are generated from DYNAMICXCF, the DYNAMICXCF_PFXLEN6 value has no meaning. The field value can be changed through the use of IPCONFIG6 statements.

DYNAMICXCF_SECCLASS

Specifies the security class for IP filtering associated with each dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of *0*. The value is used only when IPSECURITY is one of the values of the IPCONFIG field. Valid security classes are integers in the range 1 - 255. The default value is 255. The field value can be changed through the use of IPCONFIG statements.

DYNAMICXCF_SECCLASS6

Specifies the security class for IP filtering with each IPv6 dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. This value is used only when IPSECURITY is one of the values of the IPCONFIG6 field. Valid security classes are integers in the range 1 - 255. The default value is 255. The field value can be changed through the use of IPCONFIG6 statements.

DYNAMICXCF_SOURCEVIPAINT

Specifies the name of the static VIPA interface used as the source IP address when SOURCEVIPA is one of the IPCONFIG6 values and outbound packets are sent over the dynamically generated XCF or Same Host interfaces.

GLOBALCONF_IQDVLAN

Returns the VLAN ID which is used when HiperSockets (iQDIO) connectivity is used for dynamic XCF support. Valid VLAN IDs are integers in the range 1 - 4094. They are used to partition communication across HiperSockets. Stacks on the same CPC using the same HiperSockets CHPID that use the same VLAN ID can establish communications. Stacks on the same CPC using the same HiperSockets CHPID that use different VLAN IDs cannot. The field value can be changed through the use of GLOBALCONFIG statements.

GLOBALCONF_MLSCHECKTERM

Flag field that indicates whether the stack should be terminated after writing an informational message when inconsistent configuration information is discovered in a multilevel-secure environment. The field value can be changed through the use of GLOBALCONFIG statements.

GLOBALCONF_XCFGRPID

Provides a group ID value *tt* which is needed only if you want to use subplexing. If the field is not empty, *tt* is a two-digit suffix that is used in generating the XCF group name that the TCP/IP stack joins. The group name is EZBT*vvtt*, where the *vv* value is the VTAM XCF group ID suffix specified with the XCFGRPID VTAM start option.

If no VTAM XCF group ID suffix was specified, the group name is EZBTCP*tt*.

If no VTAM XCF group ID suffix is specified and GLOBALCONF_XCFGRPID is missing, the group name is EZBTCPCS.

These characters are also used as a suffix for the EZBDVIPA and EZBEPORT structure names, in the form EZBDVIPA*vvtt* and EZBEPORT*vvtt*. If no VTAM XCF group ID suffix was specified, the structure names are EZBDVIPA01*tt* and EZBEPORT01*tt*. If the GLOBALCONF_XCFGRPID field is missing, the XCF group name is EZBT*vv*CS and the structure names are EZBDVIPA*vv* and EZBEPORT*vv*. If no VTAM XCF group ID suffix was specified, the group name is EZBTCPCS and the structure names are EZBDVIPA and EZBEPORT. The field value can be changed through the use of GLOBALCONFIG statements.

IPCONFIG

The IPCONFIG field is a repeated flag field that provides information about IPCONFIG parameters. The field value can be changed through the use of IPCONFIG statements. The field can have the following values:

CLAWUSEDOUBLENOP
Channel programs for CLAW devices are forced to have two NOP CCWs to end the channel programs. It is required for some vendor devices, and applies to only first-level MVS systems.

DATAGRAMFWD NOFWDMULTIPATH
The transfer of data between networks is enabled. When transferring data between networks, if there are multiple equal-cost paths to a destination, TCP/IP uses the first active route found for forwarding each IP packet.

DATAGRAMFWD FWDMULTIPATH PERPACKET
The transfer of data between networks is enabled. In transferring data between networks, if there are multiple equal-cost routes to a destination network or host, TCP/IP, upon forwarding an IP packet to a given host in that destination network, selects a route on an approximate round-robin basis from a multipath routing list to that destination host. The selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NODATAGRAMFWD
The transfer of data between networks has been stopped by disabling IP datagram routing between different network interfaces. Forwarding is disabled.

DYNAMICXCF
Dynamic XCF support is enabled.

NODYNAMICXCF XCF
Dynamic support is not enabled.

FORMAT LONG
For stacks which are not enabled for IPv6, the command output is displayed as if it could contain IPv6 addresses. If the stack is enabled for IPv6, then the presence or absence of this value does not make any difference to the command format. FORMAT SHORT For stacks which are not enabled for IPv6, command output is displayed as if it could contain only IPv4 addresses and not the longer IPv6 addresses. If the stack is enabled for IPv6, this value is not present. This does not make any difference to the command format.

IGNOREREDIRECT
The IGNOREREDIRECT parameter was used in an IPCONFIG statement, or you are using OMPROUTE, or you are using Intrusion Detection Services (IDS) policy to detect and discard ICMP Redirects. As a result, TCP/IP ignores ICMP Redirect packets. IPSECURITY IPv4 IP filtering and IPv4 IPSec tunnel support are activated.

IQDIOROUTING
Inbound packets that are to be forwarded by the TCP/IP stack are eligible to be routed directly between a HiperSockets device and an OSA-Express device in QDIO mode without needing to be sent to this TCP/IP stack for forwarding. This type of routing over a HiperSockets device (iQDIO) is called HiperSockets Accelerator. If specified, HiperSockets Accelerator routes are created dynamically as this TCP/IP stack learns of destination IP addresses that can be routed to or from HiperSockets links without needing to be forwarded to this TCP/IP stack.

NOIQDIOROUTING
Inbound packets that are to be forwarded by this TCP/IP stack are not routed directly between a HiperSockets device and an OSA-Express device in QDIO mode. These packets are processed and routed by this TCP/IP stack.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERPACKET
Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host.

NOMULTIPATH
The multipath routing selection algorithm for outbound IP traffic is disabled. If there are multiple equal-cost routes to a destination, TCP/IP uses the first active route found to send each IP packet.

PATHMTUDISCOVERY
TCP/IP is to dynamically discover the PMTU, which is the smallest MTU of all the hops in the path. This is used to prevent fragmentation of datagrams.

NOPATHMTUDISCOVERY
TCP/IP is not to provide path MTU (PMTU) discovery support.

SOURCEVIPA
TCP/IP is to use the address present in the TCPSTACKSOURCEVIPA field (if that field is not missing) or the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams that do not have an explicit source address. If the outgoing interface was defined with the INTERFACE statement, TCP/IP uses the VIPA specified on the SOURCEVIPAINTERFACE parameter of the INTERFACE statement instead of the HOME list.

NOSOURCEVIPA
TCP/IP is not to use the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams.

STOPONCLAWERROR
Channel programs (HALTIO and HALTSIO) are stopped when a device error is detected.

SYSPLEXROUTING
The TCP/IP host is part of an MVS sysplex domain.

NOSYSPLEXROUTING
The TCP/IP host is not part of an MVS sysplex domain.

QDIOACCELERATOR
Inbound packets that are to be forwarded by this TCP/IP stack are eligible to be routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface
- Two OSA-Express QDIO interfaces
- Two HiperSockets interfaces

These packets do not need to be sent to this TCP/IP stack for forwarding. This processing behavior also applies to packets that are forwarded by the Sysplex Distributor. This type of routing is called QDIO Accelerator.

NOQDIOACCELERATOR
Inbound packets that are to be forwarded by this TCP/IP stack are not routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface.
- Two OSA-Express QDIO interfaces.
- Two HiperSockets interfaces

These packets are processed and routed by this TCP/IP stack.

IPCONFIG6

A repeated flag field that provides information on the current settings for `IPCONFIG6` configuration options. Field value for these configuration setting can be changed through the use of `IPCONFIG6` statements. Information on the following configuration settings can be included in this field.

DATAGRAMFWD NOFWDMULTIPATH
The transfer of data between networks is enabled. When transferring data between networks, if there are multiple equal-cost paths to a destination, TCP/IP uses the first active route found for forwarding each IP packet.

DATAGRAMFWD FWDMULTIPATH PERPACKET
The transfer of data between networks is enabled. In transferring data between networks, if there are multiple equal-cost routes to a destination network or host, TCP/IP, upon forwarding an IP packet to a given host in that destination network, selects a route on an approximate round-robin basis from a multipath routing list to that destination host. The selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NODATAGRAMFWD
The transfer of data between networks has been stopped by disabling IP datagram routing between different network interfaces. If the TCP/IP stack is also configured to be a sysplex distributor, datagrams destined to a sysplex-distributed dynamic VIPA are forwarded to stacks, whether or not forwarding is enabled.

DYNAMICXCF
Dynamic XCF support is enabled for IPv6.

NODYNAMICXCF
Dynamic XCF support is not enabled for IPv6 on this TCP/IP.

IGNOREREDIRECT
The `IGNOREREDIRECT` parameter was used in an `IPCONFIG6` statement, or you are using `OMPROUTE`. TCP/IP ignores ICMPv6 Redirect packets.

IGNOREREDIRECT
The `IGNOREREDIRECT` parameter was used in an `IPCONFIG6` statement, or you are using `OMPROUTE`. TCP/IP ignores ICMPv6 Redirect packets.

IGNOREROUTERHOPLIMIT
TCP/IP ignores any hop limit value received in a router advertisement from a router. The global hop limit value (configured with the `IPCONFIG6 HOPLIMIT` statement) is not overridden by the router advertisement value for all routes using the interface on which the router advertisement was received.

NOIGNOREROUTERHOPLIMIT
TCP/IP does not ignore a hop limit value received in a router advertisement from a router. This results in the configured global hop limit value being overridden by the router advertisement value for all routes using the interface on which the router advertisement was received.

IPSECURITY
IPv6 IP filtering and IPv6 IPSec tunnel support are activated.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). The `MULTIPATH` parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). The `MULTIPATH` parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which

does not provide multipath routing). The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERPACKET
Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. This field indicates that the selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NOMULTIPATH
The multipath routing selection algorithm for outbound IP traffic is disabled. If there are multiple equal-cost routes to a destination, TCP/IP uses the first active route found to send each IP packet.

SOURCEVIPA
TCP/IP is to use a virtual IP address assigned to the IP_TCPSTACKSOURCEVIPA interface (if IP_TCPSTACKSOURCEVIPA is specified) or to the SOURCEVIPAINTERFACE interface as the source address for outbound datagrams that do not have an explicit source address. If multiple addresses are assigned to the IP_TCPSTACKSOURCEVIPA interface or the SOURCEVIPAINTERFACE interface, the source address is selected from among these addresses according to the default source address selection algorithm.

SOURCEVIPA
TCP/IP is to use a virtual IP address assigned to the IP_TCPSTACKSOURCEVIPA interface (if IP_TCPSTACKSOURCEVIPA is specified) or to the SOURCEVIPAINTERFACE interface as the source address for outbound datagrams that do not have an explicit source address. If multiple addresses are assigned to the IP_TCPSTACKSOURCEVIPA interface or the SOURCEVIPAINTERFACE interface, the source address is selected from among these addresses according to the default source address selection algorithm.

NOSOURCEVIPA
TCP/IP is not to use a VIPA address as the source IP address for outbound datagrams.

TEMPADDRS
TCP/IP is to generate IPv6 temporary addresses for PAQENET6 OSA-Express QDIO interfaces for which stateless address autoconfiguration is enabled.

NOTEMPADDRS
TCP/IP should not generate IPv6 temporary addresses.

IPCONFIG_IPSECURITY

Flag field that indicates whether IPv4 IP filtering and IPv4 IPSec tunnel support have been activated. The field value can be changed through the use of IPCONFIG statements.

IPCONFIG6_IPSECURITY

Flag field that indicates whether IPv6 IP filtering and IPv6 IPSec tunnel support have been activated. The field value can be changed through the use of IPCONFIG6 statements.

IPSEC_DVIPSEC

Flag field that indicates whether IPsec tunnels associated with IPv4 dynamic VIPA addresses are eligible to be distributed if the dynamic VIPA address is being distributed. The IPsec tunnels are also eligible to be moved during dynamic VIPA takeover or giveback. The field value can be changed through the use of IPSEC statements.

IPSEC_LOGENABLE

Flag field that indicates whether logging is enabled for packet filtering. If IPSEC_LOGENABLE is true, then the following log messages might also be written to the syslog by the Traffic Regulation Manager Daemon (TRMD): EZD0814I, EZD0815I, EZD0821I, EZD0832I, EZD0833I, EZD0836I, and EZD0822I. The log setting on the individual default filter rules and the implicit default rules is honored. The field value can be changed through the use of IPSEC statements.

IPSEC_LOGIMPLICIT

Flag field that indicates whether packet filter logging is enabled for packets that are denied by the implicit default rules. IP traffic not explicitly permitted by the default IP filter rules parameters is handled by implicit default rules generated by the stack as long as the default IP filter policy is in effect. A setting of LOGIMPLICIT is honored only when filter logging is enabled on the IPSEC statement with LOGENABLE. The field value can be changed through the use of IPSEC statements.

LAST_CHANGE_DATETIME

Provides the date and time that the TCP/IP stack was last changed. The format of this field is DATETIME.

NETMON_PKTTRCSERVICE

Flag field that indicates whether the real-time TCP/IP packet trace service (SYSTCPDA) is enabled to run on the TCP/IP stack. This service enables network management applications to access trace data collected for any active packet traces or data traces. The field value can be changed through the use of NETMONITOR statements.

NETMON_SMF_IPSECURITY

Flag field that indicates whether real-time IPSec SMF record support is enabled. The field value can be changed through the use of NETMONITOR statements.

NETMON_SMF_PROFILE

Flag field that indicates whether real-time TCP/IP profile SMF event record support is enabled. The field value can be changed through the use of NETMONITOR statements.

NETMON_SMFSERVICE

Flag field that indicates whether the real-time SMF record information service (SYSCPSM) is enabled to run on the TCP/IP stack. The SMF record information service provides an interface for network management applications to obtain stack information in the form of SMF 119 records. Enabling or disabling this service has no effect on the SMF recording function that is available through separate configuration options on the SMFCONFIG profile statement or the FTP.DATA SMF configuration statements. The field value can be changed through the use of NETMONITOR statements.

NETMON_TCPCONN_MINLIFE

Specifies the minimum connection lifetime, specified in seconds, for connections reported by the TCP connection information server. The server waits for this

period before recording information about new connections. If the connection has closed in the meantime, then the connection is not reported by the TCP connection information server. If the field contains *0*, then all connections are reported. The field value can be changed through the use of NETMONITOR statements.

NETMON_TCPCONNSERVICE

Flag field that indicates whether the real-time TCP connection information service (SYSTCPCN) is enabled to run on the TCP/IP stack. The TCP connection information service provides an interface for network management applications to obtain information about TCP connections on this stack. The field value can be changed through the use of NETMONITOR statements.

SACONFIG_OSASF_PORT

A value between 1 to 65535 which indicates a port number and marks the corresponding TCP/IP instance as a candidate to communicate with OSA/SF to retrieve SNMP management data. The data comes from ATM devices and links. A value of 0 in this field indicates that the corresponding TCP/IP instance is no longer a candidate to communicate with OSA/SF, in the event that the OSA/SF-to-TCP/IP connection is restarted. The field value can be changed through the use of SACONFIGstatements.

SACONFIG_SNMP_PORT

Field specifies the port number which is used in establishing communication with the SNMP agent. For the TCP/IP SNMP subagent to communicate with the z/OS Communications Server SNMP agent, the port number specified must match the port number specified on the -p parameter when the SNMP agent is started.

SACONFIG_SNMP_PWDEFAULT

Flag field indicates whether the community name (or password) used to establish contact with an SNMP agent is public, which is the default. For the TCP/IP SNMP subagent to communicate with the z/OS Communications Server SNMP agent, the community name must match one that is defined in the PW.SRC or SNMPD.CONF data set used by the SNMP agent or specified on the -c parameter when the SNMP agent is started. The field value can be changed through the use of SACONFIG statements.

SMF119_FTPCLIENT

Flag field whether SMF type 119 records of subtype 3 are created when a user invokes the FTP client command. The field value can be changed through the use of SMFCONFIG statements.

SMF119_IFSTAT

Flag field that indicates whether SMF type 119 records of subtype 6 containing statistics related to LINK utilization are created. The field value can be changed through the use of SMFCONFIG statements.

SMF119_IPSECURITY

Flag field indicates whether SMF type 119 records of subtypes 77 and 78 are created when a dynamic tunnel is added and removed. Also, SMF type 119 records of subtypes 79 and 80 are created when a manual tunnel is activated or deactivated. The field value can be changed through the use of SMFCONFIG statements.

SMF119_PORTSTAT

Flag field that indicates whether SMF type 119 records of subtype 7 containing statistics related to reserved PORT utilization are created. The field value can be changed through the use of SMFCONFIG statements.

SMF119_TCPINIT

Flag field indicates whether SMF type 119 records of subtype 1 are created when TCP connections are established. The field value can be changed through the use of SMFCONFIG statements.

SMF119_TCPIPSTACK

Flag field that indicates whether SMF type 119 records of subtype 8 are created when a TCP/IP stack is activated and when it is terminated. The field value can be changed through the use of SMFCONFIG statements.

SMF119_TCPIPSTAT

Flag field indicates whether SMF type 119 records of subtype 5 containing TCP/IP statistics are created. The field value can be changed through the use of SMFCONFIG statements.

SMF119_TCPTERM

Flag field that indicates whether SMF type 119 records of subtype 2 are created when TCP connections are terminated. The field value can be changed through the use of SMFCONFIG statements.

SMF119_TN3270CLIENT

Flag field indicates whether SMF type 119 records of subtype 22 and 23 are created when the TSO Telnet Client code starts or ends a connection. The field value can be changed through the use of SMFCONFIG statements.

SMF119_UDPTERM

Flag field that indicates whether SMF type 119 records of subtype 10 are created when a UDP Socket is closed. The field value can be changed through the use of SMFCONFIG statements.

SYSPLEX_GROUP

Field provides the group name for the sysplex.

TCP_RESTRICTLOWPORTS

Flag field that indicates whether TCP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements. In this case, applications that have a dependency on being able to obtain an available TCP port in the 1 - 1023 range without having that port explicitly reserved for its use should be run as APF authorized or superuser. The use of RESTRICTLOWPORTS increases system security. The field value can be changed through the use of TCPCONFIG statements

TCPSTACKSOURCEVIPA

Specifies the IPv4 address used as the source IP address for outbound TCP connections. if SOURCEVIPA is one of the values of the IPCONFIG field. The address must be a static VIPA or an active dynamic VIPA (DVIPA). The field value can be changed through the use of IPCONFIG statements.

TCPSTACKSOURCEVIPA6

Specifies the name of a static VIPA or a dynamic VIPA interface. If SOURCEVIPA is one of the values of the IPCONFIG6 field and if the interface has multiple IP addresses, then the *sourcevipa* address for outbound packets is selected from

among these addresses according to the default source address selection algorithm. The field value can be changed through the use of IPCONFIG6 statements.

UDP_RESTRICTLOWPORTS

Flag field that indicates whether UDP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements. In this case, applications that have a dependency on being able to obtain an available UDP port in the 1 - 1023 range without having that port explicitly reserved for its use should be run as APF authorized or superuser. The use of RESTRICTLOWPORTS increases system security. The field value can be changed through the use of UDPCONFIG statements.

IP_VIPA: TCP/IP VIPA configuration

The IP_VIPA NEWLIST selects and reports on the VIPA (Virutal IP Address) configuration data for TCP/IP stacks. You can use the following fields to select, exclude, and list data as required. In addition to these fields, each record is uniquely identified by the following fields that are common to all TCP/IP configuration records: COMPLEX, SYSTEM, STACK, SYSNAME, SYSPLEX, and SYSTEM. For information about these fields, see "Common fields" on page 1055.

You can change the field values in the IP_VIPA NEWLIST using VIPADYNAMIC statements. For more information, see the *z/OS Communications Server: IP Configuration Guide (SC31-8776)* at http://publib.boulder.ibm.com/infocenter/zos/v1r11/topic/com.ibm.zos.r11.halz001/toc.htm.

Field descriptions

The IP_VIPA NEWLIST provides the following fields for reporting.

ACTIVE

Indicates whether the Dynamic Virtual IP address is currently active.

INTERFACE

Contains the name of the IPv6 interface.

IP

The IP field contains the Dynamic Virtual IP address (DVIPA).

IPMASK

The IPMASK field contains the IPv4 subnet mask. If the destination address is in IPV6 format, this field is missing.

OPTIONS

The OPTIONS field provides information on the following configuration settings for the VIPA.

MOVEABLE IMMEDIATE
Indicates if the dynamic VIPA whose address is present in the IP field can be activated on this TCP/IP stack if the DVIPA is not already active elsewhere in the sysplex. If the DVIPA has been activated and the TCP/IP stack where the DVIPA is defined by a VIPADEFINE statement is subsequently activated, the DVIPA is activated immediately on that TCP/IP stack. The TCP connections to this TCP/IP stack are preserved. The MOVEABLE IMMEDIATE parameter is used only for activating the DVIPA when it is not already active in the sysplex. If the DVIPA is active, this parameter is ignored.

MOVEABLE NONDISRUPTIVE
Indicates an immediate, nondisruptive movement of a dynamic VIPA from

one stack to another stack. A dynamic VIPA in the VIPARANGE statement can be moved to another stack when that stack requests ownership of the DVIPA as the stack creates it. This ownership request occurs under the following conditions:

- An application binds to the DVIPA,
- The MODDVIPA utility is used to create the DVIPA through the SIOCSVIPA or SIOCSVIPA6 ioctl.
- The application directly issues the SIOCSVIPA or SIOCSVIPA6 ioctl.

The new owning stack forwards packets for any existing connections to the original stack in order that the existing connections are not disturbed. All new connection requests are directed to the new owning stack.

CPCSCOPE
Indicates that the dynamic VIPA whose address is present in the IP field is specific to the central processor complex (CPC) on which it is defined. The VIPA is not moved to or taken over by another TCP/IP stack that is in a different CPC. A DVIPA defined with this characteristic can be used as the default route for incoming requests from Tier 1 targets on this CPC. The Tier 1 target addresses must be on the same subnet as that determined by the address mask value present in theIPMASK field.

TIER1
Indicates that the dynamic VIPA whose address is present in the IP field distributes incoming requests to non-z/OS targets like DataPower appliances or Linux hosts running on system Z.

TIER2
The TIER2 field indicates that the dynamic VIPA whose address is present in the IP field distributes incoming requests from Tier 1 targets to the group of server applications that is named.

SERVICEMGR
Indicates that sysplex distributor performs Multinode Load Balancing (MNLB) by functioning as a Service Manager in place of the Cisco LocalDirector. For these distributed dynamic VIPAs, the SERVICEMGR has no effect if a VIPADISTRIBUTE DEFINE statement does not exist for the dynamic VIPA or VIPAs. SERVICEMGR is optional and can be specified on a VIPABACKUP statement only when MOVEABLE is also specified. This parameter is only for activating the DVIPA when it is not already active in the sysplex. If the DVIPA is active when the VIPABACKUP statement is processed, this parameter is ignored.

PFXLEN

The PFXLEN field contains the prefix length of the subnet address.

RACF_ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands. The display contains userid, access, ACL id, conditional class, and the conditional profile name. The default output length is 45 characters, but the profile name can be 255 characters so the maximum output length is 290 characters.

Use the EXPLODE output modifier for a complete access list that includes access per user through each connect group. Use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use the EFFECTIVE output modifier to extend the resolved access list into the

effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE, so it works best if specified in the scope of a NEWLIST, while there are no outer selections or with the UNIVERSAL modifier specified to force collection of all relevant data. The SCOPE modifier can be used to extend the modifiers EXPLODE, RESOLVE, and EFFECTIVE with administrative access. To print the ids, the access levels, or both, the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Format names for input and output" on page 810.

RACF_PROFILE

Identifies the profile that protects the resource name identified in the RESOURCE field. The profile is programmatically derived using the current RACF database and RESOURCE as inputs.

RANK

Specifies the intended order of the Virtual IP addresses in the VIPABACKUP statement. The VIPAs are listed in their respective backup chains, relative to other stacks in those backup chains. Larger numerical rank values move the respective stacks closer to the beginning of the backup chain. Lower values indicate a position nearer to the end of the backup chain, while higher values indicate a position nearer to the beginning of the chain.

RESNAME

Contains the last qualifier of the SAF SERVAUTH resource name found in the RESOURCE field.

RESOURCE

Identifies the name of an SAF SERVAUTH resource. The resource name has the following format: EZB.MODDVIPA.*sysname.tcpname.resname*. The variable identifiers have the following meanings:

sysname is the value of the MVS &SYSNAME. system symbol. The value comes from the SYSNAME field.

tcpname is the name of the procedure used to start the TCP/IP stack. The value comes from the STACK field.

resname is the 8-character value following the SAF keyword in a SAFNAME statement. The value comes from the RESNAME field.

TYPE

Identifies the Dynamic Virtual IP address (DVIPA) entry type. This field can have the following type values:

VIPABACKUP
Designates one or more dynamic VIPAs for which this stack provides automatic backup.

VIPADEFINE
Designates one or more dynamic VIPAs that this stack should initially own and support. Other stacks can provide backup for these VIPAs if this stack fails.

VIPARANGE
Specifies whether a subnet for which dynamic VIPA activation requests are honored through a BIND, SIOCSVIPA IOCTL, or SIOCSVIPA6 IOCT operation is to be defined or deleted. The value can be *DEFINE* or *DELETE*.

JOBCLASS: JES2 Job Classes

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The JOBCLASS NEWLIST (NEWLIST TYPE=JOBCLASS) describes the job classes per MVS JES2 subsystem. each entry in this NEWLIST can be uniquely identified by the fields SYSTEM SUBSYSTEM CLASS.

Field descriptions

The JOBCLASS NEWLIST provides the following fields for reporting.

ACCT

Flag field that describes whether an account number is required on a JCL JOB statement for the current jobclass. If set (ACCT=YES), the account number is required.

AUDITCONCERN, CONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The audit concerns currently defined are listed in the following table. The AUDITCONCERN field can contain one or more concerns separated by commas.

The following audit concerns have been defined regarding Bypass Label Processing:

- BLP left to non-RACF security product

  BLP is allowed for the job class, and a security product other than RACF is active. Security zSecure does not check the BLP protection.
- BLP allowed; TAPEVOL not active, will not test ICHBLP

  BLP is allowed for the job class, but the RACF TAPEVOL class is not active. BLP is not RACF-protected. Whether the FACILITY ICHBLP resource is protected or not is irrelevant, it is not checked.
- BLP allowed; FACILITY not active

  BLP is allowed for the job class, and the RACF TAPEVOL class is active, but the RACF FACILITY class is not active. BLP is not RACF-protected.
- BLP allowed; no ICHBLP profile

  BLP is active, and the RACF TAPEVOL and FACILITY classes are active. However, no ICHBLP profile or any generic profile matching the ICHBLP resource name was defined. BLP is not RACF-protected.
- BLP allowed; UACC of ICHBLP >= UPDATE

  BLP is RACF-protected, but the UACC of the profile used is UPDATE or higher; the RACF-protection is inadequate, since most users are able to use BLP to update tapes.
- BLP allowed for input; UACC of ICHBLP >= READ

  BLP is RACF-protected, but the UACC of the profile used is READ or higher; the RACF-protection is inadequate, since most users are able to use BLP to read tapes.
- BLP RACF-protected

  BLP is RACF-protected. Security zSecure has not detected any audit concerns; the access list of the ICHBLP profile must still be checked.

The following audit concerns have been defined regarding embedded MVS commands:

– MVS Display commands allowed

  Informational MVS commands are allowed in the job class.

– MVS Modify commands allowed

  MVS console, system, or I/O commands are allowed in the job class.

These messages might be followed by one of the following:

– RACF-protected

  RACF is configured to protect the MVS commands by using profiles in the OPERCMDS class. Although there are no catchall profiles (a profile with key=*.**, key=* or key=**) defined, the default RC for this class denies access.

– RACF-protected with UACC=*access*

  RACF is configured to protect the MVS commands by using profiles in the OPERCMDS class. A catchall profile (a profile with key=*.**, key=* or key=**) exists with a UACC that provides the indicated access. The higher the access level, the higher the severity of this concern.

– RACF-protected but low OPERCMDS default RC

  RACF is configured to protect the MVS commands by using profiles in the OPERCMDS class. However, no catchall profile (a profile with key=*.**, key=* or key=**) for this class is defined, and the default RC is too low, possibly allowing access.

– not RACF-protected

  The MVS commands are not protected by RACF. The OPERCMDS class is not active or not defined in de class descriptor table.

Furthermore, these messages are followed by a verify statement:

– verified by operator

  The MVS commands are verified by the operator before being executed.

– not verified by operator

  The MVS commands are not verified by the operator before being executed. (The commands might be displayed on the console.)

Three low-priority audit concerns have been defined:

– No SMF 6

  No SMF type 6 records are written for the job class.

– No SMF 26

  No SMF type 26 records are written for the job class.

– No account numbers required

  The job class does not require account numbers.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 365. JOBCLASS NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.

Table 365. JOBCLASS NEWLIST: Audit priority values and descriptions (continued)

Priority	Meaning
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

AUTH

This field describes the AUTH parameter of the job class, which specifies the MVS command groups to be executed. The AUTH field is a text field, not a symbolic field. This value can be one or more of these text strings: SYS, IO, CONS, and INFO. If all values are set, the text string has the value ALL.

When searching for a particular value other than ALL, for example, IO, include the ALL value in your query. For example, to search for all job classes with an AUTH value including IO, specify:

```
SELECT AUTH=(:IO,ALL)
```

This example selects all AUTH values that match the string ALL or that include the string IO.

Note: When JES2 3.1.3 or later with RACF 1.9 or later is active, the AUTH parameter is ignored.

Table 366. AUTH values and descriptions

AUTH value	Meaning
ALL	All command types
CONS	Console commands
INFO	Information commands
IO	Input/output commands
MASTER	Master console
SYS	System commands

BLP

This flag field describes the Bypass Label Processing parameter of the current jobclass. If set (BLP=YES), bypass label processing is performed subject to SAF (System Authorization Facility) controls; if not set (BLP=NO), the bypass label parameter in the label field of a DD parameter will be ignored, independently of SAF controls.

CLASS

This field describes the class name (a single character).

When combined with the SUBSYSTEM and SYSTEM fields, the CLASS field uniquely identifies an entry in this NEWLIST type.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMMAND

This field describes the jobclass' command disposition parameter, which determines the action taken for MVS commands received imbedded in JCL. This field can have the following values:

Table 367. COMMAND field values and descriptions

Command value	Meaning
DISPLAY	Display the command on the console and execute it without verification.
EXECUTE	Execute the command without display or verification.
IGNORE	Silently ignore the command.
VERIFY	Have the command verified by the operator.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

HOLD

This flag field describes whether jobs in this jobclass are to be held until the operator issues a RELEASE. If set (HOLD=YES), the job is held until released.

IEFUJP

This flag field describes whether the IEFUJP exit is taken when a job is purged. If set (IEFUJP=YES), the exit is taken.

IEFUSO

This flag field describes whether the IEFUSO exit is taken when a job reaches its SYSOUT output limit. If set (IEFUSO=YES), the exit is taken.

PROCLIB

This field contains the numeric suffix used in defining the PROCLIB DD-name used for this jobclass: PROC*xx*.

REGION

This field describes the default for the region size in this job class. This field has the format **nnnn**K or **nnnn**M, specifying the region size in kilobytes or megabytes.

SUBSYSTEM, SUBSYS

This field describes the subsystem name. For more information on the subsystem, see the NEWLIST TYPE=SUBSYS.

When combined with the SYSTEM and CLASS fields, the SUBSYSTEM field uniquely identifies an entry in this NEWLIST type.

SWA

This field describes whether the SWA (Scheduler Work Area) control blocks for this jobclass are placed above or below the 16 MB line of virtual storage. The value of this field can be ABOVE or BELOW.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. This field length is 8 characters for compatibility with other NEWLIST types.

When combined with the SUBSYSTEM and CLASS fields, the SYSTEM field uniquely identifies an entry in this NEWLIST type.

TIME

This field describes the default for the maximum time that each job step runs. This field has the format *mmmm,ss* or *mmmmmm,ss*, with *mmmm* describing the time in minutes and *ss* describing the time in seconds.

TYPE6

This flag field describes whether SMF record type 6 records (JES2 Output Writer records) are to be written for the current jobclass. If set TYPE6=YES), the records are to be written.

Note: The SMF options and SMF exits determine whether the SMF record is really written. Review the SMF options and Exit reports to see whether this is the case.

TYPE26

This flag field describes whether SMF record type 26 records (JES2 Job Summary records) are to be written for the current jobclass. If set (TYPE26=YES), the records are to be written.

Note: The SMF options and SMF exits determine whether the SMF record is really written. Review the SMF options and Exit reports to see whether this is the case.

MEMBER: Library Change Detection

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The MEMBER NEWLIST (NEWLIST TYPE=MEMBER) describes physical data set members and the changes made to the members over time. There is no simple set of fields that uniquely identifies an entry in this NEWLIST type, because data sets are tracked across multiple systems and volume serials, and multiple versions. In most cases, DATASET VOLSER MEMBER NUMBER is sufficient.

For the sake of convenience, the MEMBER NEWLIST also describes the select few non-partitioned data sets for which checksum information is present in the CKFREEZE file, that is for data sets explicitly specified at CKFREEZE creation. For these data sets, only a limited number of fields in the MEMBER NEWLIST produce meaningful information. In most cases, this should be obvious from the field description. See "Field descriptions."

Field descriptions

The MEMBER NEWLIST provides the following fields for reporting.

AC1

This flag field indicates whether the Authorization Code flag is set to AC=1 or not. It is only available for load modules (LOADMOD=YES). See also the APF field.

ADDITION

This flag field indicates whether the member version is an *addition*, for example a member version was not available in the previous snapshot in which the physical data set was found. It is set for members added to a data set, but also

for a member that reappeared this snapshot after disappearing the previous snapshot, for example rename ONE to TWO and back to ONE). Because the value of this field is based on directory information, it applies only to partitioned data sets.

ALIAS

This flag field indicates whether the member is an alias of another member. Since the value of this field is based on directory information, it applies only to partitioned data sets.

ALIAS_OF

This text field indicates the name of the base member if the current member is an alias. For example, if PROGALIS is an alias of BASE, the ALIAS_OF field in PROGALIS is set to BASE, and the ALIAS_OF field in BASE is blank. It is only available if the ALIAS field is set.

AMODE

This field contains the addressing mode of the load module. It will be **24**, **31**, **64**, or **ANY**. It is only available for load modules (LOADMOD=YES).

APF

This flag field indicates whether the data set is APF-authorized in the most-recent snapshot for each of the systems the data set is found on. A data set is APF-authorized when it appears on the APF list, on the LPA list or on the linklist if it is authorized. If the data set is APF-authorized on at least one system, the APF flag is set.

APPL

This field contains the application owning the load module. It is based on a guess, using a prefix of the member name, and might be wrong in some cases. It is empty if no guess could be made.

BYTES

This field indicates the member size on disk, in kilobytes. It is only available if the CKFREEZE file used was produced with the CHECK=Y orCHECKDSN=*datasetname* parameter specified. For sequential data sets, this field indicates the amount of data contained in the data set, again in kilobytes.

CHECKSUM

This field contains the TEXT checksum on the current member version. It is a 4-byte hexadecimal number (8 characters). The TEXT checksum is a simple checksum based on member contents. It is the same for the same member on any system, independent of the site and CHECKPWD, member name, PDS directory information, ISPF statistics, IDR and ZAP data, etc. It is not very safe against malicious attacks; see the CRC field for a safe checksum. It is only available if the CKFREEZE file used was produced with the CHECK=Y or CHECKDSN=*datasetname* parameter specified.

The main use of the TEXT field is to identify duplicate copies of the member, possibly with another member name or in another data set. The safe CRC checksum, which is dependent on the member name, checksum, etc., cannot be used for this purpose. For sequential data sets, this field can be used to determine whether two entire data sets have identical contents.

COMPLEX

This repeated field describes the security complex that contains the system. This might come from an ALLOC COMPLEX parameter or default to a system name.

CRC

This field contains the CRC checksum on the current member version. It is a 4-byte hexadecimal number (8 characters). The CRC checksum is a digital signature that is safer than the TEXT checksum in that it is very hard for changes to go undetected. In addition, it is different for each site and each CHECKPWD, making it hard for a virus to circumvent the CRC. It is only available if the CKFREEZE file used was produced with the CHECK=Y or CHECKDSN=*datasetname* parameter specified. This field applies to sequential data sets too.

DATASET, DSN

This field describes the data set name.

DELETION

This flag field indicates whether the member version is a *deletion*, for example if a member version is not available in the next snapshot in which the physical data set is found. Because Security zSecure does not report on a member that is not there, the deletion flag is set in the last member version in which the member does appear. It is set for members renamed or deleted from a data set. Since the value of this field is based on directory information, it applies only to partitioned data sets.

DSORG

This field provides an indication of the type of data set. Possible values are PDS, PDSE, PS (indicating normal physical sequential), TAPE, LDS, and ESDS (the last two being VSAM subtypes). Using an overriding output length of less than 4 will result in less distinction, with possible values of PO, PS, and VS only. This field cannot be used on SELECT/EXCLUDE statements.

ENDDATE

This field describes the last snapshot (CKFREEZE) date during which the version was unchanged. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see “Date fields” on page 903.

EPA

This field contains the Entry Point offset of the load module. It is only available for load modules (LOADMOD=YES).

IDENTIFY

This repeated field contains the identify data for the member version, in the format '**Date Description**'. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the IDENTIFY_ID and NEW_IDENTIFY fields.

IDENTIFY_ID

This repeated field contains the identify ids for the member version, in the format '**Description**'. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the IDENTIFY and NEW_IDENTIFY fields.

LAST_CHANGE

This field indicates the date and time when the member was last changed or when it was created, whichever is more recent. If the current member version belongs to a PDSE data set and has extended member statistics, this field provides the extended member statistics. Otherwise, this field provides PDF statistics information for the member which includes the PDF_CHGDATE and PDF_CHGTIME, or the PDF_CREADATE, respectively. For information on using this field in SELECT and EXCLUDE operations, "Combined date and time fields" on page 904.

LAST_CHANGE_USERID

This field indicates the user ID that was last used to modify the member. If the current member version belongs to a PDSE data set and has extended member statistics, this field provides the user ID taken from the extended member statistics. Otherwise, this field provides the user ID taken from the PDF statistics for the member. (See "PDF_USERID" on page 1098.)

LKEDDATE

This field describes the date the member was link-edited. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

LOADMOD

This flag field indicates whether the member is a load module. If set (LOADMOD=YES), the load-module related fields APPL, STORSIZE, EPA, AC1, RENT, REUS, OL, NX, SSI, and AMODE are also available. If not set (LOADMOD=NO), the load-module related fields are left blank.

MEMBER

This field describes the member name.

NEW_IDENTIFY

This repeated field contains the identity data for the member version, in the format '**Date Description**'; unlike the IDENTIFY field, it includes only the IDENTIFY data that was not available in the previous member version. If the current version is 1 (NUMBER=1), this will be empty. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the IDENTIFY and IDENTIFY_ID fields.

NEW_ZAP

This repeated field contains the AMASPZAP IDRDATA for the member version, in the format '**Date Description**'; unlike the ZAP field, it includes only the ZAP data that was not available in the previous member version. If the current version is 1 (NUMBER=1), this will be empty. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the ZAP and ZAP_ID fields.

NUMBER

This field describes the current version number. This number is 1 for the first version found, and is equal to the VERSIONS field for the last version found. The value of this field depends on the CHECK/CHECKDSN parameters that were in effect when the CKFREEZE was created: without CHECK=YES (or at least CHECKDSN for the data sets you want to report about), certain changes might go undetected.

NX

This flag field indicates whether the module is Not Executable. It is only available for load modules (LOADMOD=YES).

OL

This flag field indicates whether the module is Only Loadable. It is only available for load modules (LOADMOD=YES).

PDF

This flag field indicates whether PDF statistics are available for the member. If set (PDF=YES), the related PDF_xx fields are also available. If not set (PDF=NO), the related PDF_xx fields are left blank.

PDF_CHGDATE

If the current member version has PDF statistics, this field describes the date the member was last changed. If no PDF statistics are available, this field is left blank. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

PDF_CHGTIME

If the current member version has PDF statistics, this field describes the time the member was last changed, in the format 'HH:MM'. If no PDF statistics are available, this field is left blank.

PDF_CREADATE

If the current member version has PDF statistics, this field describes the date the member was created. If no PDF statistics are available, this field is left blank. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

PDF_USERID

If the current member version has PDF statistics, this field describes the user who last modified the member. If no PDF statistics are available, this field is left blank.

PDF_VERSION, PDF_VVMM

If the current member version has PDF statistics, this field describes the version and modification level in the format 'VV.MM'. If no PDF statistics are available, this field is left blank.

PREVDATE

This field describes the previous version's enddate, for example the last snapshot (CKFREEZE) date during which the previous member version was unchanged. It is not available if the NUMBER field is 1. The change occurred in the period PREVDATE to STARTDATE. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

PSIGNED

This flag field indicates whether the signed attribute bit is set or not in the library directory entry for the module. This attribute is available only for load modules in a PDSE.

PSIGPROB

This flag field indicates whether or not program signature verification failed for the module. This attribute is available only for load modules in a PDSE.

RENT

This flag field indicates whether the module is re-entrant. It is only available for load modules (LOADMOD=YES).

REUS

This flag field indicates whether the module is serially reusable. It is only available for load modules (LOADMOD=YES).

RMODE

This field contains the residency mode of the load module. It is **24** or **ANY**. It is only available for load modules (LOADMOD=YES).

SCAN_INSTR

This field describes the result of an *instruction scan* performed on the member. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and CHECK=Y or CHECKDSN=*datasetname* parameter specified. The instruction scan is performed on the full length of the member, and checks for suspicious instructions in the code.

Note: You should use the contents of this field as a warning, not as a certainty. The instruction scan can cause false alarms and might also be fooled to miss certain instructions. You should always review the source code of suspicious modules.

When used for select/exclude processing, you can use SELECT SCAN_INSTR or SELECT SCAN_INSTR=ANY to select routines in which *any* specified instruction was found; use SELECT SCAN_INSTR=NONE to select routines in which no specified instructions were found. In addition, you can select routines containing any of the specific instructions listed in the following table, for example, SELECT SCAN_INSTR=(FAKEAPF,FAKESPEC).

Because many suspicious instructions can be found within a single module, the default output of this field is in a condensed format; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 9, for example SCAN_INSTR(EXPLODE,9). The following table lists the SCAN_INSTR values that can be used for SELECT/EXCLUDE processing; the condensed output; the exploded output; and the meaning.

Table 368. SCAN_INSTR values available for SELECT/EXCLUDE processing

Select/Exclude	Condensed	Exploded	Meaning
BYPASS BYPASSSAF	.B.....	BypassSAF	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	FakeAPF	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	FakeOper	Set operations authority
FAKEPRIV	......P	FakePriv	Set privileged/trusted authority
FAKESPEC	....S..	FakeSpec	Set special authority
KEYZERORB	...0...	KeyzeroRB	For an SVC: modify caller's RB to key-zero
MODESUPRB	..M....	ModeSupRB	For an SVC: modify caller's RB to supervisor mode

Note: The values printed by the SCAN_INSTR field are subject to change. Do not write applications that are dependent on the output of this field.

SCAN_STRING

This field describes the result of a *string scan* performed on the member. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter, SCANSTR arguments, and CHECK=Y or CHECKDSN=*datasetname* parameter specified. The string scan is performed on the full length of the member, and checks for user-specified strings in the code.

By default, zSecure Collect scans load modules for an instruction sequence that is indicative of a published leak. If you have not added another scan string to the Collect run, if the module resides in an APF library and has AC1, and this field returns Yes, then you probably have a big leak in the system.

The value of this field is set to **Yes** if a matching string was encountered in the code; **No** if no string was found; the field is left blank if no string scan was performed.

SCAN_SVC

This repeated field describes the result of an SVC*scan* performed on the member. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter, SCANSVC list of SVC numbers, and CHECK=Y or CHECKDSN=*datasetname* parameter specified. The SVC scan is performed on the full length of the member, and checks for user-specified SVC calls in the code.

Note: You should use the contents of this field as a warning, not as a certainty. The SVC scan might cause false alarms, and can also be fooled to miss certain SVC calls. You should always review the source code of suspicious modules.

The value of this field has the format '**num: description**' if the SVC scanned for was one of the first seven specified in zSecure Collect; if any of the other SVCs scanned for was encountered, this field has the value '**Other**'.

SEQUENTIAL

This flag field indicates that the data set is not a partitioned data set, but one of the following types of data sets: physical sequential (either tape or DASD), VSAM LDS, or VSAM ESDS.

SMSPLEX, SYSPLEX

This field describes the sysplex name, as specified in SYS1.PARMLIB member COUPLExx.

SSI

This hexadecimal field describes the SSI data. It is only available for load modules (LOADMOD=YES).

STARTDATE

This field describes the first snapshot (CKFREEZE) date during which the version was unchanged. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see “Date fields” on page 903.

STORSIZE

This field contains the in-storage size of the load module, in kilobytes. It is only available for load modules (LOADMOD=YES).

SYSTEM

This repeated field describes the systems on which the physical data set was found for this member version.

TTR

This field describes the member TTR, as a 3-byte hexadecimal number (6 characters). For a PDS, this is the track (TT, two bytes) and record number (R, 1 byte) in the data set where the member starts.

VERSIONS

This field describes the number of versions found for the current member. This number will be 1 if the member was unchanged in all observations. To select on members that changed, use SELECT VERSIONS>1. The value of this field depends on the CHECK/CHECKDSN parameters that were in effect when the CKFREEZE was created: without CHECK=YES (or at least CHECKDSN for the data sets you want to report about), certain changes might go undetected. If you read "data set" for all occurrences of "member" in the previous paragraph, the text applies to sequential data sets too.

VOLSER, VOLUME

This field describes the volume serials on which the physical data set was found for this version.

ZAP

This repeated field contains the AMASPZAP IDRDATA for the member version, in the format '**Date Description**'. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the ZAP_ID and NEW_ZAP fields.

ZAP_ID

This repeated field contains the AMASPZAP IDRDATA for the member version, in the format '**Description**'. It is only available if the CKFREEZE file used was produced with the IDR=YES parameter specified or implied. See also the ZAP and NEW_ZAP fields.

MERGE: RACF Database Merge

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•			

The `MERGE NEWLIST (NEWLIST TYPE=MERGE)` provides information about merge processing decisions made during RACF Database Merge operations. This NEWLIST is only available if database merge processing is active. All decisions taken during merge processing are logged, with a reference to the command type, the decision type, the merge phase, and the ids involved. This information provides the data to create reports on the effect of each merge command, pass, and merged profile. No reports have yet been designed.

In this report type, each record describes one decision made, a choice between two default groups for a specific user ID for example. The number of records generated for each profile is dependent on the type of field:

- Fields that describe user/group structure generate one record per user/group and field, even if the value of the field did not change: SUPGROUP, DFLTGRP, OWNER.
- Fields that describe security attributes generate one record per user/group and field, but only if the value of the field changed: SPECIAL, group-SPECIAL, etc.
- All other fields grouped together generate one record per profile.

The MERGE report does not include information about fatal errors during merge processing. These errors are reported through structured error messages.

Field descriptions

The MERGE NEWLIST provides the following fields for reporting.

CLASS, C

This field contains the class name of the profile described by this record. It can be USER, GROUP, DATASET, CONNECT (which is also valid for restructured databases), or a general resource class name, such as TAPEVOL.

CODE

This numeric field returns further information as to why a decision was made. Its meaning depends on the PASS in which the decision was made. Note that several of its values are undocumented here, as these are used for internal bookkeeping and generating error messages. As a consequence, these values will never show up in your reports. The values that can show up are:

Pass 2:	1:	The specified MERGERULE RENAME will be used in further processing.
Pass 3:	1:	The specified MERGERULE SUPGROUP will be used.
	2:	The source superior group is not selected; use the current superior group.
	4:	This group is source-only, and its superior group is not selected. However, the superior group exists on the current system and will be used without modification.
	5:	This group is source-only, so we use its superior group.
	6:	Source and current superior group are identical.
Pass 4:	1:	Use the specified MERGERULE OWNER.
	3:	This profile is current-only; use the current owner.
	5:	Use this group's superior group as the new owner.
	6:	This profile is source-only; use the source owner.
	7:	Source and current owners are the same.
	9:	The owner of this profile has been renamed and will be used as the new owner.
Pass 5:	1:	Use the applicable MERGERULE CONNECT.
Pass 6:	1:	Use the applicable MERGERULE to determine the default group.
	2:	The source default group is not selected; the current one will be used.
	3:	This user is source-only; use the source default group.
	4:	This user is source-only, and the source default group is not selected. The owner will be used as the new default group.
	5:	The source and current default group are identical.
	9:	This user is source-only, its default group is not selected, and the owner cannot be used either. Fortunately, exactly one connect is copied for this user; that group will be used as the default group.
	10:	The default group has been renamed and will be used as the new default group.
Pass 7:	1:	Use the applicable MERGERULE DATA to determine the owner.
	2:	Source and current owners are identical.
	3:	No MERGERULE DATA has been specified. The current owner will be used.
	4:	This profile is source only. The source owner will be used.
	5:	This profile is source-only. The High-level qualifier of the profile will be used as the new owner.
Pass 8:	1:	The appropriate MERGERULE AUTHORITY will be used.

Pass 10:	4:	This AUTHORITY-related field has been set because of a MERGERULE.
	5:	This AUTHORITY-related field has been set because the profile is source-only.

CUR_PROFILE

This field contains the new (current) name of the profile described by this record. It is the same as the original (source) profile name, which is described by the SRC_PROFILE field, unless the profile was renamed. See also the PROFILE field.

CUR_VALUE

This field contains the current value of the field described by this record. See also the SRC_VALUE and NEW_VALUE fields.

FIELD

This field contains the name of the profile field described by this record. It can be a name from the templates or a connect subfield name.

NEW_VALUE

This field contains the new value of the field described by this record, that is, the value that the field should have according to the merge. See also the SRC_VALUE and CUR_VALUE fields.

PASS

This numeric field contains the pass in which the decision was made. It can have a value in the range 2 to 10. The numbers 2 through 9 refer to passes CKRMRG2...CKRMRG9; a short description of their purpose appears in the SYSPRINT. The number 10 corresponds to CKRMRGC, the pass in which the commands are generated.

PROFILE

This field contains the name of the profile described by this record. If the profile is not renamed, it contains a single value. If the profile is renamed, it is a repeated field, containing both the original (source) profile name and the new (current) profile name. See also the SRC_PROFILE and CUR_PROFILE fields.

REASON

This field returns a short description of the reason why a particular decision has been made. Its main purpose is to be of help in pinpointing the cause of unwanted resulting commands.

SRC_PROFILE

This field contains the original (source) name of the profile described by this record. It is the same as the new (current) profile name, which is described by the CUR_PROFILE field, unless the profile was renamed. See also the PROFILE field.

SRC_VALUE

This field contains the original (source) value of the field described by this record. See also the CUR_VALUE and NEW_VALUE fields.

MOUNT: UNIX Mount Points

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The MOUNT NEWLIST (NEWLIST TYPE=MOUNT) describes what file systems are mounted on what mount points. For information about the file system content, see "UNIX: UNIX System Services File System" on page 1480.

Each record in this NEWLIST represents a mount point (on a system). A record can be uniquely identified by the fields SYSTEM, COMPLEX and MOUNTPOINT. An alternate key is SYSTEM, COMPLEX and DEV.

Field descriptions

The MOUNT NEWLIST provides the following fields for reporting.

ACL

Flag field that indicates if the file system supports ACLs. This field can have the following values:

- *Yes* indicates that the file system supports ACLs.
- *No* indicates that the file system does not support ACLs.
- The field is blank if the file system does not recognize ACLs.

In a sysplex environment with some systems that support ACLs and some that do not, files with ACLs are inaccessible from downlevel systems that do not recognize ACL functionality if the FSSEC class is active on an up level system. The files might be accessible by the owner or superuser.

AGGREGATESIZE

The size in blocks of the aggregate. Normally the number of blocks that fit in the primary allocation.

AUDITCONCERN, CONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs. The content of the field is subject to change. The AUDITCONCERN field might contain one or more concerns separated by commas. The following audit concerns have currently been defined:

- Disk scavenging threat / not C2 compliant

  The New Block Security (NBS) option of the ZFS aggregate is inactive. If this option is inactive, it means that if the system crashed while extending or creating a file, and the user data has not yet made it to the disk, the data to be overwritten on disk might be read by anyone who has read access to the extended or newly created file. This situation potentially provides unauthorized users with access to sensitive data in the ZFS. This setting is also a direct violation of the requirements for a C2 rating according to the Orange Book.
- HFS filesystem does not contain security labels

  An HFS file system does not support security labels. If the SETROPTS MLFSOPJ option is activated, the best option is to migrate your file systems to ZFS.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 369. MOUNT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

BLOCKSIZE

The size of a block of a zFS file system in bytes (normally 8192 bytes).

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

Contains the name of the viewpoint security complex. This value can be specified by the COMPLEX= keyword on an explicit ALLOC statement, or it can default to a system name.

DEV, DEVICE

Contains the device number, which identifies the file system from a viewpoint system.

DSN, DSNAME, DATASET

The MVS data set name of the file system associated with the MOUNTPOINT. This value might not be directly accessible from SYSTEM. See "OWNING_SYSTEM" on page 1106.

FILESYSNAME

The name of the file system. For most file systems, this name is equal to the dataset name.

FILESYSTYPE

Type of file system as specified on the FILESYSTYPE keyword for the BPXPRM*xx* parmlib member. The value is either *HFS* or *TFS* (temporary file system).

FRAGMENTSIZE

Size of a fragment of the zFS file system in bytes. Multiple files can share a logical block if they are smaller than (block size - fragment size), in which case the block gets split up in fragments. The size of a fragment can range from 1024 up to the block size.

MODE

This field indicates how the file system is mounted, read-only or in read/write mode.

MOUNTPOINT

Absolute pathname for the file system root.

NBS

New Block Security. This option only applies to zFS file systems. When enabled, disk blocks are physically cleared before they are linked to a file.

OWNING_COMPLEX

This field contains the name of the security complex of which the system that owns the file system data set associated with the mount point is a part. See also "OWNING_SYSTEM."

OWNING_SYSTEM

Contains the name of the system that owns the file system data set associated with the mount point. The unified file system within a sysplex can be shared. If it is shared, the actual data set can be managed by one system while providing access to all systems even if the systems do not share the DASD.

READONLY_SECLABEL

Contains the security label that is assumed for UNIX file systems (z/OS 1.5 and up) if all of the following conditions are met:

- The security product running on the system is RACF.
- The data set for the file system is protected by a DATASET profile that specifies a security label.
- The file system is mounted read-only.
- The SETROPTS MLFSOBJ option is active when you mount the file system.
- The root directory of the file system does not have a security label.

See also 1460, and "SECLABEL" on page 1489.

RWSHARE

A flag field that indicates whether the zFS read-write file system is sysplex-aware. If the value is Yes, the zFS file system is mounted with SYSPLEX_MODE=on or mounted with PARM(RWSHARE) when SYSPLEX_MODE=filesys. If the value is No, the zFS file system is not sysplex-aware.

SECURITY

Flag field that indicates whether the file system is mounted with the SECURITY option that determines whether security checks are performed. If this option is not active, the setuid, setgid, APF, and program control bits are ignored. For directories, the sticky bit is also ignored if the SECURITYoption is not active.

SERIAL

Describes the volume serial number for the DASD unit and the device ID for the file system data set associated with the mount point. This field might not return a value if the CKFREEZE data sets that have been allocated do not contain a detailed description of both the OWNING_SYSTEM and the SYSTEM. This field can be used to disambiguate between DASD volumes with the same volume serial. See also "BOX_SERIAL field for DASDVOL report" on page 1014 for further details.

SETUID

Flag field that indicates whether the file system is mounted with the SETUID option that determines if the setuid, setgid, APF, and program control bits are

to be honored. The file system must also be mounted with the SECURITY option for these bits to actually be honored. See "SECURITY" on page 1106.

SYSPLEX_MODE

A field that indicates the sysplex status. The possible values are:

- **Noshare**: zFS is not in a shared file system environment.
- **Admin-only**: zFS is in a shared file system environment but is not sysplex-aware.
- **On**: zFS is in a sysplex-aware environment with sysplex=on.
- **Filesys**: zFS is in a sysplex-aware environment with sysplex=filesys.

SYSTEM

The name of the (viewpoint) system. For MVS systems, this value is the SMF system ID. The field length is 8 characters by default for compatibility with other NEWLIST types.

TRUSTED

Flag field that indicates if the file system is mounted as trusted or not. This field indicates if the setuid, setgid, program control and APF authorized bits are honored. It summarizes the SECURITY and SETUID flags.

VOLSER, VOLUME

The first volume serial of the file system data set associated with the mount point. This field might not have a value if the CKFREEZE data sets that are allocated do not contain a detailed description of the OWNING_SYSTEM and the SYSTEM.

MSG: Message Processing Facility

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The MSG NEWLIST (NEWLIST TYPE=MSG) describes the message-specific data of the MVS Message Processing Facility (MPF). Each entry in this NEWLIST can be uniquely identified by the fields SYSTEM MSGID.

Field descriptions

The MSG NEWLIST provides the following fields for reporting.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas. The following audit concerns have currently been defined:

- RACF message suppressed

  RACF is active, and a RACF message is suppressed. Security messages should not be suppressed; if too many such messages occur, they should be routed to a separate console.
- Default messages suppressed

  The default-entry .NOENTRY is suppressed. All messages not explicitly named in the MPF table are suppressed.

- Message automated

  The message is automated. This is not a serious concern, though the automation should be reviewed.
- Message suppressed

  The message is suppressed. This is not a serious concern, though the message id should be checked to see whether the message is sensitive and should not be suppressed.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 370. MSG NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

AUTO

This field indicates the automation setting specified for the message. It is set to NO if the message is not eligible for automation processing and to YES if it is but no automation token was specified. Otherwise it will contain the token that will be passed to the automation subsystem.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

EXIT

This field indicates the module name of a user exit defined for the message. If no user exit is defined, the EXIT field and the derived fields are blank.

EXIT_ADDRESS

This field indicates the address of the user exit defined for the message. See also the EXIT field.

EXIT_AT

This field indicates the load module information for the user exit defined for the message. See also the EXIT field. It contains a short description of the program name, module name, and offset, in the format described in the following table.

Table 371. EXIT_AT format description

EXIT_AT format	Minor/Major EP	Offset zero
Module	Major	Yes
Module+offset	Major	No
Program in Module	Minor	Yes
Program+offset in Module	Minor	No

EXIT_WHERE

A string indicating the virtual storage area where the exit routine resides. Possible EXIT_WHERE values and their meaning are documented in the following table. The areas starting with an E reside above the 16 MB line in virtual storage.

Table 372. EXIT_WHERE values and descriptions

EXIT_WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

MPFLST

The parmlib member name of the member used to set MPF processing.

MSGID

The message id, a string of up to 10 characters. When combined with the SYSTEM field, the MSGID field uniquely identifies an entry in the NEWLIST TYPE=MSG.

SUPPRESS, SUP

This text field indicates whether the message is suppressed. If a message is suppressed (SUPPRESS=YES), the message is not displayed on the MCS console. If SUPPRESS=ALL, not only is the message not displayed, the command responses are suppressed as well.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. When combined with the MSGID field, the SYSTEM field uniquely identifies an entry in the NEWLIST TYPE=MSG.

NEWLIST: Report translation properties

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The NEWLIST TYPE=NEWLIST enumerates the non-suppressed `NEWLIST` statements encountered when a CARLa program is run and lists the original English and default translated properties for each `NEWLIST` type included in the program.

An approximate key for records in this `NEWLIST` type is `NEWLIST_TYPE NEWLIST_NAME SRCEDDN SRCEMEM SRCELINE`, but it is not necessarily unique.

Table 373 list the fields supported by the `NEWLIST TYPE=NEWLIST`.

Table 373. `NEWLIST TYPE=NEWLIST` - available fields.

Field Name	Column Header	Length
"DETAILHELPPANEL" on page 1111	**Det help panel**	8
"HELPPANEL" on page 1111	**Help pnl**	8
"LANGUAGE" on page 1111	**Lng**	3
"NEWLIST_NAME" on page 1111	**Name**	16
"NEWLIST_TYPE" on page 1111	**Type**	24
"SRCEDDN" on page 1111	**DDname**	8
"SRCELINE" on page 1111	**Line**	6
"SRCEMEM " on page 1111	**Member**	8
"SUBTITLE" on page 1111	**Subtitle**	64
"SUBTITLE_ORIG" on page 1111	**Original subtitle**	64
"SUMHELPPANEL" on page 1111	**Sum help panel**	8
"TITLE" on page 1111	**Title**	64
"TITLE_ORIG" on page 1111	**Original title**	64
"TOPTITLE" on page 1111	**Toptitle**	64
"TOPTITLE_ORIG" on page 1111	**Original toptitle**	64

Field descriptions

The NEWLIST NEWLIST provides the following fields for reporting.

DETAILHELPPANEL

The identifier for the help panel associated with the detail panel opened using a DISPLAY command.

HELPPANEL

The identifier for the help panel associated with the overview of panel showing selected records that is opened using a DISPLAY command.

LANGUAGE

The specified translation language for the NEWLIST output. This value is a three-character abbreviation for the language as defined in a LANGUAGE statement.

NEWLIST_NAME

The NAME passed on the NEWLIST statement. This value is optionally suffixed with .DISPLAY if the NEWLIST statement contains a DISPLAY or DSUMMARY statement, as opposed to only a subset of the LIST, SORTLIST, and SUMMARY statements.

NEWLIST_TYPE

The character format for the NEWLIST.

SRCEDDN

The ddname where the NEWLIST statement was encountered.

SRCELINE

The line number where the NEWLIST statement was encountered.

SRCEMEM

The member name where the NEWLIST statement was encountered (if the ddname is not unique).

SUBTITLE

The final subtitle for this NEWLIST.

SUBTITLE_ORIG

The original text for the subtitle. This value has not been translated.

SUMHELPPANEL

The identifier for the help panel associated with the summary level display panel opened using the DISPLAY command.

TITLE

The final title for this NEWLIST If translation is specified, this value represents the translated title.

TITLE_ORIG

The original text for the title. This value has not been translated.

TOPTITLE

The final top-level title for this NEWLIST. If translation is specified, this value represents the translated title.

TOPTITLE_ORIG

The original text for the top-level title. This value has not been translated.

PC: Program Calls

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The PC NEWLIST (NEWLIST TYPE=PC describes program calls that are identified by system-table-entry. Each Program Call entry is a record in this NEWLIST type which means that, for all entries in a table, the table-related information is the same.

Use a SUMMARY command to display the table-related information. Information that is repeated for the table is repeated for each entry in the PC report or listing. One possible example of repeated information is the LX field.

Each entry in this NEWLIST can be uniquely identified by the fields SYSTEM ENTRY EX.

Field descriptions

ADDRESS

Contains the address of the program call routine as 32 bit address. Several program calls can share the same address. Also, a Program Call that does not use space-switching that resides in private storage might execute different code depending on the address space for the caller. Each address space can create its own version in private storage.

ADDRESS64

Contains the address of the program call routine as 64 bit address. Several program calls can share the same address. Also, a Program Call that does not use space-switching that resides in private storage might execute different code depending on the address space for the caller. Each address space can create its own version in private storage. See also "ADDRESS."

AKM

Contains a 4-digit hexadecimal number with the Authorized Key Mask, which is a 16-bit bit field representing the list of PSW keys that the caller can have. The value X'8000' indicates key-0, value X'0001' indicates key-15. The AKM_KEY field lists the individual keys from the AKM.

AKM_KEY

Repeated field that contains the list of PSW keys that the caller can have. Together these keys form the Authorized Key Mask AKM, representing the PSW keys the caller can have. Each key is a decimal number in the range 0 to 15.

AMODE

Contains the addressing mode of the program call routine. The value can be **24**, **31**, or **64**.

ASID

Contains the ID of the address space in which the program call routine executes. If this program call routine is not a space-switching program call

(SPACE_SWITCH=NO), this field is blank, indicating the current address space. The address space ID is a 2 byte hexadecimal number; the JOBNAME field shows the related job name.

AT

Repeated field that contains a short description of the program name, module name, and offset, in the format described in the Table 374. The values are derived from the program-call address.

Table 374. AT format description

AT format	Minor/Major EP	Offset zero
Module	Major	Yes
Module+offset	Major	No
Program in Module	Minor	Yes
Program+offset in Module	Minor	No

AUDITCONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your program because the content might change. The AUDITCONCERN field can contain one or more concerns separated by commas. The following audit concerns have currently been defined:

- **In caller's private area**

  The Program Call is executed in the private area of the caller, and the Program Call is available in more than one address space. Each address space can execute different code for the Program Call. If the Program Call is available to unauthorized callers, and executes authorized or with additional authorization, any user might be able to subvert the system.
- **Caller may be unauthorized**

  The Program Call is available to non-authorized callers.
- **LPA param in writable storage**

  The Latent Parameter Area contains a value that, if used as a pointer, points to writable common storage. This situation potentially permits all users to alter the parameters to the Program Call.
- **Executes authorized**

  The Program Call executes in authorized state. For BASIC program calls, this configuration is normal.
- **Resides in common storage**

  The Program Call resides in common storage, hence a risk of disassembly.
- **System Entry Table**

  Available to callers in all address spaces.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 375. PC NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.

Table 375. PC NEWLIST: Audit priority values and descriptions (continued)

Priority	Meaning
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

AUTHREQ

Flag field that indicates if authority is required to use the Program Call. That is, if the AKM contains key 8. If set (AUTHREQ=YES), authority is required.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can come from the ALLOC COMPLEX parameter or default to a system name.

CONTENT, CONTENTS

A string containing up to the first 256 bytes of the routine, which usually include the eye catcher. The default output length of this string is 128 characters (containing the first 128 bytes of the program call routine). In the default output format, the readable text from the contents is shown; the non-printable parts of the contents have been replaced by one or two periods (.).

DESCRIPTION, SFT_DESCRIPTION

This character field contains a description of the Program Call. If the program call routine is a system-defined program call routine as indicated by definition of the SFT_INDEX field, this value is a description of the entry in the System Function Table. In other cases, zSecure tries to guess the function using the module name. If a description is found, it is printed in parentheses (SMS) for example, which indicates that the name is a guess and might be incorrect. If the product cannot make a guess about the module name, the field is left blank.

EK

Contains the PSW protection key that the program call routine uses for running the routine if this value is set by the program call.

EKM

Contains a 4-digit hexadecimal number with the Entry Key Mask EKM of the program call routine. The value X'8000' indicates key-0, value X'0001' indicates key-15. Depending on the PKM field, this key mask is ORed with the key mask for the caller (PKM=OR) or replaces the key mask for the caller (PKM=REPLACE). The EKM_KEY field lists the individual keys from the EKM.

EKM_KEY

Repeated field that contains the list of PSW keys that make up the Entry Key Mask EKM of the program call routine. Depending on the PKM field, this key mask is ORed with the key mask for the caller (PKM=OR) or replaces the key mask (PKM=REPLACE).

ENTRY

Contains a number identifying the Entry Table which the program call routine is a part of. When combined with the SYSTEM and EX fields, this value uniquely identifies a program call routine.

This field has the same value for all Program Call routines that are part of the same entry table.

Note: This field is *not* system-defined, it is defined by Security zSecure to distinguish between entry tables.

ET_ASID

Contains the ID of the address space owning the Entry Table.

All Program Call routines that are part of the same entry table have the same value in this field.

ET_CONNECTS

This field contains the number of connections for the Entry Table.

All Program Call routines that are part of the same entry table have the same value in this field.

ET_JOBNAME

This field contains the job name of the address space owning the Entry Table. If no job name can be found, this field has the format '>ASID<', where ASID represents the address space ID.

All program call routines that are part of the same entry table have the same value in this field.

ET_SYSTEM

Flag field that indicates if the Entry Table that the program call routine is a part of is a system table (`ET_SYSTEM=YES`) or not. A system table defines `PC` routines that can be called from any address space.

All Program Call routines that are part of the same entry table have the same value in this field.

EX

Contains the index in the Entry Table that identifies the program call routine. When combined with the SYSTEM and ENTRY fields, this value uniquely identifies a program call routine. The entry index EX is a decimal field of up to three digits.

JOBNAME

Contains the job name of the address space in which the program call routine runs. If this program call routine does not use space-switching (`SPACE_SWITCH=NO`), this field is blank, indicating the current address space. If no job name can be found, this field has the format '*>ASID<*', where `ASID` represents the address space ID.

KEY

This field contains the storage protection key of the Program Call routine, if it resides in CSA, ECSA, SQA, or ESQA.

In current systems, a storage key of 8 or 9 is a serious cause for concern because any user is able to change the Program Call routine. A key of 10 to 15 is a

minor cause for concern: Only users executing in that key are able to change the Program Call routine. Keys 10 to 15 can normally only be used by applications running programs from APF libraries. An exception exists for ADDRSPC=REAL. For additional information see 1451.

LENGTH

Contains the length of the program or module that the Program Call is part of if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, or PLPA). If the CKFREEZE data contains sufficient information, this value can also indicate if the residency is a server address space private area (PVT, EPVT). The length is approximated as the length up to the end of the module, or the length up to the next entry point.

LX

Repeated field that contains the Linkage Index numbers for the Entry Table that identifies the program call routine. It is part of a structured repeat group with information such as address space ID, *dormant flag*, and so on.

All Program Call routines that are part of the same entry table have the same value in this field. MVS tries to keep the LX for each entry table the same across all connected address spaces, but this configuration is not a hardware requirement.

LX_ASID_CNT

Repeated field that contains the number of address space IDs for the current Linkage Index repeat-group entry. This field is part of the structured repeat group described by the LX field.

All program call routines that are part of the same entry table have the same value in this field.

LX_CONN_ASID

This repeated field contains the connected address space ID for the current Linkage Index repeat-group entry. It is part of the structured repeat group described with the LX field. The address space id is a 2-byte hexadecimal number; the LX_CONN_JOBNAME field shows the related job name.

All program call routines that are part of the same entry table have the same value in this field.

LX_CONN_JOBNAME

This repeated field contains the job name of the connected address spaces for the current Linkage Index repeat group entry. It is part of the structured repeat group described with the LX field. If no job name can be found, this field has the format '>ASID<', where ASID represents the connected address space id.

All program call routines that are part of the same entry table have the same value in this field.

LX_DORMANT

This repeated flag field indicates whether the current Linkage Index repeat group entry is dormant. It is part of the structured repeat group described with the LX field.

All Program Call routines that are part of the same entry table have the same value in this field.

LX_OWNR_ASID

Repeated field that contains the owning address space ID for the current Linkage Index repeat group entry. This field is part of the structured repeat group described with the LX field. The address space id is a 2-byte hexadecimal number; the LX_OWNR_JOBNAME field shows the related job name.

All program call routines that are part of the same entry table have the same value in this field.

LX_OWNR_JOBNAME

Repeated field that contains the job name of the owning address spaces for the current Linkage Index repeat group entry. This field is part of the structured repeat group described with the LX field. If no job name can be found, this field has the format '>ASID<', where ASID represents the connected address space ID.

All program call routines that are part of the same entry table have the same value in this field.

LX_SEQNUM

Repeated field that contains the sequence number for the current Linkage Index repeat-group entry. This value is part of the structured repeat group described with the LX field. When it is nonzero, it is used to check whether the PC instruction was indeed intended to call this instance of a reused LX.

All Program Call routines that are part of the same entry table have the same value in this field.

LX_SYSTEM

This repeated flag field indicates whether the current Linkage Index repeat group entry is a system Linkage Index. It is part of the structured repeat group described with the LX field.

All Program Call routines that are part of the same entry table have the same value in this field.

LX_TABLE_CNT

This repeated field contains the number of entry tables for the current Linkage Index repeat group entry. It is part of the structured repeat group described with the LX field.

All Program Call routines that are part of the same entry table have the same value in this field.

MODE_SUP

This flag field indicates whether the program call routine executes in supervisor state (MODE_SUP=YES) or problem-program state (MODE_SUP=NO). When used for output in the default format, it is blank if MODE_SUP=NO. See also the STATE field.

Basic Program Call routines often execute in supervisor state because otherwise the Program Call cannot return to a supervisor mode program. The PR instruction cannot go from problem program mode to supervisor mode. For non-basic Program Call routines, the Program Call must only run in supervisor state if authorized operation is required.

MODULE

Contains the major entry point name of the module in which the Program Call is located, if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA,

PLPA). If CKFREEZE contains sufficient information, it can also be filled in if the residency is a server address space private area (PVT, EPVT).

OFFSET

Contains the offset between the entry point for the program and the entry point for the program call, if the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA). If the CKFREEZE data contains sufficient information, the field might also indicate if the residency is a server address space private area (PVT, EPVT). The offset is calculated from the previous entry point, and is zero if the address is located at a minor or major entry point.

PARM_ADDRESS

Contains the address of the latent parameter area for the program call routine. This area, which is typically located in ESQA, can contain one or two user-pointers determined by the creator of the Program Call. See the PARM_xx, PARM1_xx, and PARM2_xx fields.

PARM_KEY

This field contains the storage protection key of the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA. A key of 8 to 15 is a cause for concern because any user can potentially change the Latent Parameter Area.

PARM_SUBPOOL

Contains the storage area subpool of the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA.

PARM_WHERE

Contains the residency of the Program Call's Latent Parameter Area. See the WHERE field for a reference.

PARM1_ADDRESS

Contains the address of the first user parameter in the Latent Parameter Area (LPA) for the program call routine.

PARM1_AT

Contains the module information of the first user parameter in the LPA. See the AT field for a reference.

PARM1_KEY

Contains the storage protection key of the first user parameter in the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA. A key of 8 to 15 might be a cause for concern.

PARM1_SUBPOOL

Contains the storage area subpool of the first user parameter in the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA.

PARM1_WHERE

Contains the residency of the first user parameter in the Latent Parameter Area. See the WHERE field for a reference.

PARM2_ADDRESS

Contains the address of the second user parameter in the Latent Parameter Area for the program call routine.

PARM2_AT

Contains the module information of the second user parameter in the LPA. See the AT field for a reference.

PARM2_KEY

Contains the storage protection key of the second user parameter in the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA. A key of 8 to 15 might be a cause for concern.

PARM2_SUBPOOL

Contains the storage area subpool of the second user parameter in the Latent Parameter Area (LPA), if it resides in CSA, ECSA, SQA, or ESQA.

PARM2_WHERE

Contains the residency of the second user parameter in the Latent Parameter Area. See the WHERE field for a reference.

PC

Repeated field that describes the PC number, for example LX + EX. This value is the Program Call number as encountered in program code. It is part of the structured repeat group described with the LX field.

This field has the same value for all Program Call routines that are part of the same entry table.

PC_TYPE

Indicates the type of Program Call routine. The value is either `BASIC` or `STACKING`. Stacking routines are the best option.

PKM

Indicates the use made of the execution key mask (EKM). Depending on the value of the PKM field, the key mask for the caller is ORed with the EKM (PKM=OR) or replaced by the EKM (PKM=REPLACE).

PROGRAM

Indicates the 8-character name of the program that is called by the Program Call. This value is not necessarily at offset 0, nor is it necessarily the load module name; it might be a minor entry point name. See field AT for a more accurate (but wider) field that includes any nonzero offset and both major and minor names, if available.

SCAN_INSTR

Describes the result of an *instruction scan* performed on the Program Call code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter. The instruction scan is performed on the full length of the Program Call (not just on the eye catcher) and checks for suspicious instructions in the code.

Note: Interpret the contents of this field as a warning, not as a certainty. The instruction scan can cause false alarms, and can also be fooled to miss certain instructions. Always review the source code of suspicious modules.

When used for SELECT or EXCLUDE processing, you can use SELECT SCAN_INSTR or SELECT SCAN_INSTR=ANY to select routines in which *any* specified instruction was found; use SELECT SCAN_INSTR=NONE to select routines in which no specified instructions were found. In addition,

you can select routines containing any of the specific instructions listed in the table Table 376, SELECT SCAN_INSTR=(FAKEAPF,FAKESPEC) for example.

Because many suspicious instructions can be found within a single module, the default output of this field is in a condensed format. Full output can be split into several lines by using the EXPLODE output modifier and an overriding length of 9, SCAN_INSTR(EXPLODE,9) for example. Table 376 lists the SCAN_INSTR values that can be used for SELECT/EXCLUDE processing; the condensed output; the exploded output; and the meaning.

Table 376. SCAN_INSTR values for SELECT and EXCLUDE processing

Select/Exclude	Condensed	Exploded	Meaning
BYPASS BYPASSSAF	.B.....	BypassSAF	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	FakeAPF	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	FakeOper	Set operations authority
FAKEPRIV	......P	FakePriv	Set privileged/trusted authority
FAKESPEC	....S..	FakeSpec	Set special authority
KEYZERORB	...0...	KeyzeroRB	For an SVC: modify RB for the caller to key-zero
MODESUPRB	..M....	ModeSupRB	For an SVC: modify RB for the caller to supervisor mode

Note: The values printed by the SCAN_INSTR field are subject to changes in future releases. Do not write applications that are dependent on the output of this field.

SCAN_STRING

Describes the result of a *string scan* performed on the Program Call code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSTR arguments set. The string scan is performed on the full length of the Program Call not just on the eye catcher. The scan checks for user-specified strings in the code.

The value of this field is set to *Yes* if a matching string was encountered in the code. The value is *NO* if no string was found; the field is left blank if no string scan was performed.

SCAN_SVC

Repeated field that describes the result of an SVC*scan* performed on the Program Call code. It is only available if the `CKFREEZE` file used was produced with the `SCAN=YES` parameter and `SCANSVC` list of SVC numbers set. The SVC scan is performed on the full length of the Program Call not just on the eye catcher. The scan checks for user-specified SVC calls in the code.

Note: Interpret the contents of this field as a warning, not as a certainty. The SVC scan can cause false alarms, and can also be fooled to miss certain SVC calls. Always review the source code of suspicious modules.

The value of this field has the format `num: description` if the SVC scanned for was one of the first seven specified in zSecure Collect. If any of the other SVCs scanned for was encountered, this field has the value *`Other`*.

SFT_INDEX

If the Program Call routine is a system-defined Program Call routine, this field describes the entry number of the routine in the System Function Table. Otherwise, the field is blank. See also the DESCRIPTION field.

SPACE_SWITCH

Flag field that indicates if the Program Call routine is a space-switching call (SPACE_SWITCH=YES) or a local call (SPACE_SWITCH=NO).

STATE

Field that indicates whether the Program Call routine executes in supervisor state (STATE=SUPERVISOR) or problem program state (STATE=PROBLEM). See also the MODE_SUP field.

SUBPOOL

Contains the storage area subpool of the Program Call routine, if the residency is in CSA, ECSA, SQA, or ESQA.

SYSTEM

The name of the system. For MVS systems, this value is equal to the SMF system id. This field is 8-characters long for compatibility with other NEWLIST types.

When combined with the ENTRY and the EX fields, the SYSTEM field uniquely identifies an entry in this NEWLIST type.

WHERE

A string indicating the virtual storage area where the program call routine resides. Table 377 lists the possible WHERE values and their meaning. Areas starting with an E reside above the 16 MB line in virtual storage.

Table 377. PC NEWLIST - WHERE field values

WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

PPT: Program Properties Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The PPT NEWLIST (`NEWLIST TYPE=PPT`) describes the MVS Program Properties Table. Each entry in this `NEWLIST` represents one PPT entry, and is uniquely identified by the fields `PROGRAM SYSTEM`.

Field descriptions

The `PPT NEWLIST` provides the following fields for reporting.

AUDITCONCERN, CONCERN

This field indicates the reason for the audit priority. You should not use the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas. If a concern results from the IBM supplied IEFSDPPT for the specific OS level, the AUDITCONCERN is suffixed with the text "(IBM default)", and the AUDITPRIORITY is adjusted. The following audit concerns are currently defined:

- Bypasses SAF.

  Data set accesses by the program are not subject to SAF (System Authorization Facility) security checks. This might be very dangerous if the program can be called by arbitrary users and be induced to read from or write to user-specified data sets. Bypassing SAF is a direct violation of the B1 security policy. If B1 policy is specified such violation is indicated by a suffix of " / not B1 compliant" and high audit priority.
- Executes in system key .

  The task runs in a system key. This authorizes the task to bypass system security.
- No data set integrity

  This option turns off all data set serialization once the program is started. For instance, data sets used by the program can be deleted by another program while being used; this might mean the task can be brought down by accident.
- Modified from IEFSDPPT.

  The PPT entry was modified from the system default.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 378. PPT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

BYPASS

Flag field that indicates if DFSMS (DFP) will bypass SAF (System Authorization Facility) calls. If set, data set accesses by the program are not subject to security checks by RACF.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

DEFAULT

Flag field that indicates if the current entry is a default PPT entry. It is set for entries derived from the IEFSDPPT load module, and not set for entries set by parmlib member SCHEDxx.

HONOR_IEFUSI_REGION

Flag field that indicates if a program is to honor region size restrictions specified in MVS exit IEFUSI. The values that can be returned are:

Yes
The program honors a region size limit set in IEFUSI.

No
The program honors a region limit set in IEFUSI.

This setting is only available in z/OS Version 1 Release 10 and later. No value is returned for systems running earlier z/OS releases.

KEY

The storage protection key in which the program (job step) runs, if one was assigned. This is a decimal number in the range 0 to 15. If no storage key was assigned, this field is left blank. Keys in the range 0 to 7 imply system authorization.

NODSI

Flag field that indicates if the program requires data set integrity. If set (NODSI=YES), the program does not hold an enqueue for data sets allocated in batch (the NODSI parameter does not apply to dynamic allocations). The lack of enqueues can cause problems with data management procedures that might (re)move the data set while it is being used by the program that has NODSI.

NONCANCEL

Flag field that indicates if the program can be cancelled or not. If set (NONCANCEL=YES), the program cannot be cancelled with an MVS CANCEL command. In that case, the program can only be cancelled using the FORCE ARM command.

NONSWAP

Flag field that indicates the program is to be swappable or not. If set (NONSWAP=YES), the program is marked non-swappable.

PRIV

Flag field that indicates if the program executes privileged or not. If set (PRIV=YES), the address space in which the program is running is not swapped unless it is in a long wait state.

Note: This field should not be confused with the RACF TRUSTED or PRIVILEGED attributes.

PROGRAM

The name of the program. When combined with the SYSTEM field, this field uniquely identifies an entry in the NEWLIST TYPE=PPT.

SYSTASK

Flag field that indicates if the program is a system task. If set (SYSTASK=YES), the program is a system task and is not timed. (In this case, it must be a one-step job started by a START or MOUNT command.)

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. When combined with the PROGRAM field, this field uniquely identifies an entry in the NEWLIST TYPE=PPT.

RACF: RACF profiles

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•		

The RACF NEWLIST (NEWLIST TYPE=RACF) provides information about the RACF profiles in the database. Unlike the other NEWLIST types, the available fields are not fixed, but depend on the templates in the RACF database, which determine the layout and contents of the profiles in the database. This topic describes the fields available in supported RACF releases. In addition to the RACF template fields, some fields are added by zSecure, and you can define custom fields for this NEWLIST.

A number of standard defined variables for RACF profiles are also provided in the SCKRCARL library member C2RXDEF1, which is included in the user interface as well as in certain batch jobs. These defined variables are also documented in this topic.

You can list the database templates available on your system by issuing the TEMPLATE primary command, or by selecting the TEMPLATE option from the **AU.S - RACF** control menu option. See "TEMPLATE - Template field properties" on page 284.

In the RACF NEWLIST, the fields COMPLEX CLASS KEY SEGMENT PROFTYPE VOLSER uniquely identify an entry. An alternate key is COMPLEX DB RBA.

For performance reasons, profiles are normally stored in RACF databases in segments and not as a single record. However, RACF databases prior to V1.9.2 and non-RDS RACF databases do not necessarily follow this practice. The records returned by the RACF NEWLIST type are these profile segments, not entire profiles. If you only want to list basic profile information, include the SEGMENT=BASE option in your selection statement. This option suppresses extra lines for the other segments and only shows the profile class and key.

You can combine information from different segments into one line with a lookup operation. For example, to combine a user default account from the TSO segment with the user name from the BASE segment, include the option SEGMENT=TSO in your selection and PGMRNAME in the output specification. Conversely, you can select on a base segment property and then do a lookup to an application segment.

Note: The LIST command generates output while reading each record to conserve storage, and therefore does not support lookup operations.

Another way of combining information from different segments is to use a MERGELIST statement. The separate NEWLIST statements within the MERGELIST can then separately select and format the BASE, TSO, and other segments. If you sequence the statements according to class and key, the output for each profile is written on consecutive lines.

Table 379 lists the predefined segment types:

Table 379. RACF Profiles: Predefined segment types

Segment type	Entity types
CDTINFO	GENERAL (CDT)
CERTDATA	GENERAL (DIGTCERT and DIGTRING)
CICS	USER
DCE	USER
DFP	GROUP, USER, DATASET
DLFDATA	GENERAL (DLFCLASS)
EIM	USER, GENERAL (FACILITY and LDAPBIND)
ICSF	GENERAL (CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY)
KERB	USER, GENERAL (REALM)
LANGUAGE	USER
LNOTES	USER
NDS	USER
NETVIEW	USER
OMVS	USER, GROUP
OPERPARM	USER
OVM	GROUP, USER
PROXY	USER, GENERAL (FACILITY and LDAPBIND)
SESSION	GENERAL (APPCLU)
SIGVER	GENERAL(PROGRAM)
SSIGNON	GENERAL (PTKTDATA)
STDATA	GENERAL (STARTED)
SVFMR	GENERAL (SYSMVIEW)
TME	GROUP, GENERAL (ROLE), DATASET
TSO	USER
WORKATTR	USER

For information about the RACF NEWLIST fields available for reporting, see "Field descriptions" on page 1126.

In the RACF NEWLIST, custom field names can be defined in the CFIELD class. For user and group resource profiles, the custom field values are in the CSDATA segment. If you use these fields in a SELECT statement, explicitly specify the class (USER or GROUP) and SEGMENT=CSDATA. The fields CSCNT, CSTYPE, CSKEY, and CSVALUE are never interpreted as custom fields, but are always interpreted as representing the actual fields in the CSDATA segment. If you define custom fields using these names, you can access the fields by using the CUSTOM_DATA field or the statement SUBSELECT CUSTOM_DATA. See "CUSTOM_DATA" on page 1157.

Custom fields use the default formats, depending on the CFDTYPE field as defined in the CFDEF segment of the CFIELD profiles and loaded into the dynamic parse table. Table 380 lists the default formats. See "Format names for input and output" on page 810 for additional information on these formats.

Table 380. RACF Custom fields - default formats

Format	Description
CFDTYPE	Default
CHAR	Character
NUM	Numeric
HEX	Hexadecimal
FLAG	A $YESNO format

Field descriptions

The RACF NEWLIST provides the following types of fields for reporting.

ACL

This repeated field can be used to display the access and conditional access lists of a profile. It can only be used for output on the SORTLIST, DISPLAY, and (D)SUMMARY commands (use the fields listed with ACLCNT and ACL2CNT for SELECT/EXCLUDE processing). This field is found in GROUP, DATASET, and GENERAL profiles; in group profiles, it does not contain useful information.

The display contains userid, access, ACL id, conditional class, and conditional profile name. The default output length is 45, but since it contains a profile name that can be up to 255 characters, the maximum output length of the ACL field is 290 characters. Use the EXPLODE output modifier for a complete access list including access per user through each connect group; use the RESOLVE output modifier for a resolved access list showing the highest access of each user or group. Use EFFECTIVE to extend the resolved access list into the effective one, which also includes access due to operations or group operations. Be aware that connect information is needed for RESOLVE, EFFECTIVE and EXPLODE, so it works best if specified in the scope of a NEWLIST, while there are no outer selections or with the UNIVERSAL modifier specified to force collection of all relevant data. The SCOPE modifier can be used to extend EXPLODE/RESOLVE/EFFECTIVE with administrative access.

To display only selected repeat group entries, the DEFINE SUBSELECT command can be used. See "Subselect clauses" on page 755. To select on specific combinations of values per repeat group entry, the SELECT ACL(...) command can be used. See "SELECT/EXCLUDE ACL(...)" on page 890. For a list of access level see Table 304 on page 877.

To print just the ids or the access levels or both the ACLACCESS, ACLID and ACLIDACCESS formats can be used. See "Specifying syntax for RACF command input" on page 810.

Warning: This field should *not* be combined with the USERID field to list user/group entries. The ACL and USERID fields might have a different sort order and a different number of entries. If you want to show user- or group-related information next to an ACL field, use the ACL field as a base field, ACL:PGMRNAME for example.

ACL2ACC

For GENERAL profiles: the access level in a conditional access list, access list entries listed in the ACL2NAME, ACL2UID, ACL2ACNT, and ACL2RSVD fields. The number of conditional access list entries is listed in the ACL2CNT field. The preferred interface to this field is the ACL combination field.

ACL_ALTER

Variable defined in C2RXDEF1 that lists the ACL ids with `ALTER` access.

ACL_CONTROL

Variable defined in C2RXDEF1 that lists the ACL IDs with `CONTROL` access.

ACL_EXECUTE

Variable defined in C2RXDEF1 that lists the ACL IDs with `EXECUTE` access.

ACL_NONE

Variable defined in C2RXDEF1 that lists the ACL IDs with `NONE` access.

ACL_OPER

Variable defined in C2RXDEF1 that lists the ACL IDs with `ALTER-O` access; that is, access if provided through the `OPERATION` or group-`OPERATIONS` attributes.

ACL_READ

Variable defined in C2RXDEF1 that lists the ACL IDs with `READ` access.

ACL_UPDATE

Variable defined in C2RXDEF1 that lists the ACL IDs with `UPDATE` access.

ACL2ACNT

For GENERAL profiles: the number of access events for each entry in a conditional access list. This number is only updated for discrete profiles, and only if statistics are on (due to SETROPTS STATISTICS). This is a repeated field that can be combined with the ACL2NAME, ACL2UID, ACL2ACC, and ACL2RSVD fields. The number of conditional access list entries is listed in the ACL2CNT field.

ACL2CNT

This field lists the number of conditional access list entries. For DATASET profiles, the PROGRAM, USR2ACS, PROGACS, PAS2CNT, and ACL2VAR fields list the entries and access. For GENERAL profiles, the ACL2NAME, ACL2UID, ACL2ACC, ACL2ACNT, and ACL2RSVD fields list the entries and access. The preferred interface to this field is the ACL combination field.

ACL2NAME

For GENERAL profiles: the indicator byte in a conditional access list. This is a repeated field that can be combined with the ACL2UID, ACL2ACC,

ACL2ACNT, and ACL2RSVD fields. The number of conditional access list entries is listed in the ACL2CNT field. The preferred interface to this field is the ACL combination field.

ACL2RSVD

For GENERAL profiles: the conditional data in a conditional access list, containing class and profile name. This is a repeated output-only field that can be combined with the ACL2NAME, ACL2UID, ACL2ACC, and ACL2ACNT fields. The number of conditional access list entries is listed in the ACL2CNT field. The preferred interface to this field is the ACL combination field.

ACL2UID

For GENERAL profiles: the user or group in a conditional access list. This is a repeated field that can be combined with the ACL2NAME, ACL2ACC, ACL2ACNT, and ACL2RSVD fields. The number of conditional access list entries is listed in the ACL2CNT field. The preferred interface to this field is the ACL combination field.

ACL2VAR

For DATASET profiles, reserved field which forms part of a conditional access list entry. This is a repeated output-only field that can be combined with the PROGRAM, USER2ACS, PROGACS, and PAS2CNT fields. The number of conditional access list entries is listed in the ACL2CNT field. The preferred interface to this field is the ACL combination field.

ACLCNT

This field is found in DATASET, group and general profiles. For DATASET and general resource profiles, it lists the number of access list entries. For user profiles, it lists the number of users connected to a group. The entries are listed in the USERID, USERACS, and ACSCNT fields. The preferred interface to this field is the ACL combination field for DATASET and general resource profiles or the CONNECT combination field for group profiles. For a group with the universal attribute, this field counts only the users with higher than default authority to the group. To see the total number of users, use the CONNECT_COUNT field.

ACSALTR

This numeric field (a decimal number of up to 5 digits) is found in DATASET and GENERAL profiles. It indicates the number of times the data set or resource was successfully accessed with ALTER authority. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

ACSCNT

This field is found in DATASET, GROUP, and GENERAL profiles. It is a repeated field that can be combined with the USERID and USERACS field. The ACLCNT field lists the number of entries.

For group profiles, this field has no meaning. For DATASET and GENERAL profiles, this field lists the number of times an access list entry was used. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

ACSCNTL

This numeric field (a decimal number of up to 5 digits) is found in DATASET and GENERAL profiles. It indicates the number of times the data set or resource

was successfully accessed with CONTROL authority. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

ACSREAD

This numeric field (a decimal number of up to 5 digits) is found in DATASET and GENERAL profiles. It indicates the number of times the data set or resource was successfully accessed with READ authority. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

ACSUPDT

This numeric field (a decimal number of up to 5 digits) is found in DATASET and GENERAL profiles. It indicates the number of times the data set or resource was successfully accessed with UPDATE authority. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

ADSP

This field is an alias for the FLAG1 field found in USER BASE segments (and non-RDS CONNECT profiles). It indicates whether the user has the system-ADSP (or group-ADSP, resp.) attribute. It can be specified as an attribute, e.g. SELECT ADSP. Its opposite for the purpose of SELECT/EXCLUDE processing is NOADSP.

If the user has the ADSP attribute, a discrete profile is created every time the user creates a permanent DASD or tape data set. If assigned at the group level (in a CONNECT profile), ADSP is only in effect when that group is the user's current connect group. The ADSP attribute is only used if system-ADSP is in effect (due to SETROPTS ADSP). This is indicated by the ADSP field of NEWLIST TYPE=SYSTEM.

On standard userid overviews, this field is usually shown as the first position in a group column headed AG (ADSP and GRPACC).

ANY_CERT

Variable defined in C2RXDEF1 that is true for a userid that has at least one digital certificate. By default it displays *C* when true and blanks otherwise.

ANY_CLAUTH

Variable defined in C2RXDEF1 that is true for a userid that has class authorization in any class. By default it displays *C* when true and blanks otherwise.

ANY_GROUP_SOA

Variable defined in C2RXDEF1 that is true for a userid that has the any of the following group attributes: `SPECIAL`, `OPERATIONS`, or `AUDITOR`. By default it displays *g* when true and blanks otherwise.

ANY_LINK

Variable defined in C2RXDEF1 that is true for a userid that has any RACLINK associations. By default it displays *L* when true and blanks otherwise.

ANYSUPGROUP

This field is only found in group profiles and is a repeat group showing all superior groups. The order is from nearest to SYS1.. This field result in two passes through the database and can only be used on UNLOAD files, not on the live RACF database.

APPLDATA

This field is only found in GENERAL profiles and contains application data. This data is used by various applications, for instance by IMS, and zSecure Command Verifier.

Because APPLDATA can be used by both applications from IBM and other vendors, RACF command processing cannot validate the data. Because misspellings typically result in *not* applying the requested setting, zSecure Admin and Audit verifies a number of well-documented APPLDATA values. If a user changes the value of an APPLDATA field on an ISPF panel and that value is not recognized by zSecure Admin and Audit, a panel is presented prompting the user to select a documented value for the field or to keep the modified value specified.

In addition, an audit concern is generated for unrecognized values.

Table 381 shows which text string is recognized in which profile. APPLDATA fields can contain more text than the text to enable the setting. The strings are recognized when they are separated from any other text by blanks.

Table 381. Recognized APPLDATA value per class / profile

Class	Profile	Recognized APPLDATA value
CSFSERV / CSFKEYS	Any	RACF-DELEGATED
PTKTDATA	Any	NO REPLAY PROTECTION
FACILITY	IRR.PGMSECURITY	BASIC ENHANCED ENHANCED-WARNING
TIMS / GIMS	Any	REVERIFY

For digital certificates the APPLDATA field contains the userid associated with the certificate. For selection ease the field CERTIFICATE_ID can be used instead, which is equal to APPLDATA for the class DIGTCERT, and absent for all other classes.

ASSIZEMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum address space region size. It lies between 10,485,760 and 2,147,483,647.

ASYMUSAGE

See “CSFAUSE” on page 1154.

AUDIT

This flag field is found in DATASET and GENERAL profiles and indicates the audit flags set by the owner. These flags determine whether to log successful and failed accesses. The audit qualifiers determine the level from which accesses are logged; these are listed in the AUDITQF and AUDITQS fields. See also the GAUDIT field, which lists the audit flags set by the auditor. The easiest way to print the audit info is through the AUDITLVL, AUDITS, or AUDITF fields. Use the AUDITLVL field for modifiable displays.

The following table lists the AUDIT values and their meanings.

Table 382. Audit flag values and descriptions

AUDIT value	Meaning
ALL	Audit successful accesses from AUDITQS and failed accesses from AUDITQF.
SUCCESS	Audit successful accesses from AUDITQS.
FAILURE	Audit failed accesses from AUDITQF.
NONE	No auditing.

AUDITCONCERN, CONCERN

This field returns a concatenation of audit concerns for the profile. The following table shows the default audit priority for active and non-active classes and lists the audit concern. The table sorts audit concerns by highest audit priority without a policy statement.

Table 383. Audit priorities and concerns by class

Active class	Non-active class	Audit concern
30	30	Can logon without password
25	25	UNIX security labels are bypassed
20		Generic not active
15	1	Class not in CDT
15	1	Class not in router table
15	1	Possibly misspelled APPLDATA
11	1	Warning mode does not prevent access
10	1	Range table ignores profile
10	1	Verify why UACC>=UPDATE
10	1	UNIX ID sharing not protected because UACC greater than or equal to read
6	6	Program control inactive
6	1	Generic chars in discrete key
6	1	Generic chars in discrete member
6	1	No replay protection
4	4	Global access checking inactive
4	4	Profile not used because no such class
4	4	Profile ignored
4	1	Profile not used for access control
4	n/a	Profile probably not used because it is not RACLISTed.
n/a	1	Profile not effective
1	1	Class inactive

The priority is 40 if the concern is not compliant to the policy that has been selected. A priority of 0 means the concern is not issued unless the policy has explicitly been requested.

The following audit concerns have been defined:

Can logon without password

The userid is authorized to logon (not PROTECTED), but has no password and does not need to supply an OIDCARD either. Therefore, the userid can be used to logon without proper authentication.

UNIX security labels are bypassed

Defining the BPX.SAFFASTPATH profile in the FACILITY class causes z/OS UNIX to bypass RACF in some cases to improve performance, and you should not bypass RACF in a multilevel-secure environment.

Generic not active

This is a generic profile but its class is active and does not have generics activated. This means that this profile is not used for access checking. This could lead to unprotected data.

Class not in CDT

The class to which this profile belongs is not defined in the Class Descriptor Table. Any authority check for this profile results in a return code of 4 (profile not found) from RACF. Most applications grant access in this situation.

Class not in router table

The class to which this profile belongs is not found in the router table, which means that RACROUTE requests result in a *not protected* return code. Most applications grant access in this situation. On z/OS V1R6 and higher systems the router table is optional, and this audit concern is no longer generated.

Possibly misspelled APPLDATA

This concern is explained in detail in the APPLDATA field description.

Warning mode does not prevent access

This profile is in warning mode, which means that every access request is successful, though logging is done for each access that is not specifically granted through other means. This function should only be used temporarily while determining which access is necessary to the data protected by this profile.

Range table ignores profile

This profile does not fall within any of the ranges defined in the Range Table, so RACF is not able to use it for access control.

Verify why UACC>=UPDATE

A UACC value greater than update is extremely unusual because it grants almost unlimited access to all users. Do not specify this value unless absolutely necessary.

UNIX ID sharing not protected because UACC greater than or equal to read

Users that have access to the SHARED.IDS profile in the UNIXPRIV class and haveUPDATE access to the UID or GID fields, are able to use the SHARED keyword of the RACF ADDUSER, ALTUSER, ADDGROUP and ALTGROUP commands, allowing him or her to create users or groups using already existing user and group IDs. This new user or group has access to all the resources the already existing user or group has access to which is potentially dangerous.

Program control inactive

This profile belongs to the PROGRAM class, indicating that it contains a program that should be protected by RACF. However, program control is not active so RACF does not have any control over the access to this program.

Generic chars in discrete key

In these cases, the profile contains the actual asterisk or percent sign, instead of the internal representation used by RACF for generic profiles. Generally, these profiles are a result of errors, such as trying to define a generic profile before the class is enabled for generic profiles. The profiles can be deleted after turning generic command processing off for the class using the command SETROPTS NOGENCMD(*class*) NOGENERIC(*class*).

Generic chars in discrete member

This profile contains generic characters in its discrete member list. This is usually the result of an error.

No replay protection

The PTKTDATA profile specifies that `PassTickets` validated by the key in the SIGNON segment can be used multiple times. Only use this function in secure environments where access to generated `PassTickets` is limited within a secure or internal network. The use of `PassTickets` is still more secure than the use of normal passwords, as `PassTickets` are only valid during a 10 minute interval.

Global access checking inactive

This profile belongs to the GLOBAL class, indicating that it contains a definition for global access to be allowed for the class described by the profile. However, global access checking for that class is inactive, so this definition is not used.

Profile not used because no such class

This profile belongs to the GLOBAL class, indicating that it contains a definition for global access to be allowed for the class described by the profile. However, this class does not exist, so the definition is not used.

Profile ignored

This profile belongs to a member class that is not supposed to contain profiles, and which does not use profiles.

Profile not used for access control

For any one of a variety of reasons, this profile is not used for access control. This could lead to unprotected data.

Profile probably not used because not raclisted
A profile in an active class that has the RACLIST required property is not RACLISTed. This conditionally replaces the existing audit concern 'Profile not used for access control' (which is retained if the class is inactive).

Profile not effective
This profile belongs to an class that must be active but that has a function different from access checking, while the class in inactive. This is shown instead of the concern 'Profile not used for access control' because the class is not used for access control.

Class inactive
The class to which this profile belongs is inactive, so this profile is never used for access control.

AUDITF

This derived field contains the AUDIT(FAILURES) level. It is based on the raw AUDIT and AUDITQF fields. The possible values are listed in the following table. The blank (X'FF') value means that failure auditing is not active. It is meant for use in SELECT statements. Use the AUDITLVL field for modifiable displays.

Table 384. AUDITF values

AUDITF value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
(blank)	FF

AUDITLVL

This field is found in DATASET and GENERAL profiles; it contains the audit level (both successes and failures) in a three-character format: a success level, a blank, and a failures level. The audit levels can have the values blank (not set), 'R' (READ), 'U' (UPDATE), 'C' (CONTROL), and 'A' (ALTER). It is the only modifiable audit field.

AUDITOR

This field is an alias for the FLAG6 field found in USER BASE segments. It indicates whether the user has the system-auditor attribute. It can be specified as an attribute, SELECT AUDITOR for example. Its opposite for the purpose of SELECT/EXCLUDE processing is NOAUDITOR.

On standard userid overviews, this field is usually shown as the last position in a group column headed SOA which represents the SPECIAL, OPERATIONS, and AUDITOR attribute settings.

This field returns the audit priority for the profile. See field AUDITCONCERN for a table with the concerns and their priorities. The actual audit priority can be higher because of a SIMULATE POLICY C2 statement for example.

AUDITQF

Flag field that indicates the audit failure qualifier. This field is found in `DATASET` and general profiles.

If the `AUDIT` field is set to *ALL* or *FAILURE*, all failed accesses with intended access equal or higher than this field are logged. The `AUDITQF` field is unpredictable when failure auditing has not been specified. Use `AUDITF` instead. Use the `AUDITLVL` field for modifiable displays.

The `AUDITQF` values are listed in the following table.

Table 385. AUDITQF values

AUDITQF value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01

Table 385. AUDITQF values (continued)

AUDITQF value	Internal value (hex)
READ	00
NONE	FF

AUDITQS

Flag field that indicates the audit success qualifier. This field is found in DATASET and general resource profiles.

If the *AUDIT* field is set to *ALL* or *SUCCESS*, all successful accesses with intended access equal or higher than this field are logged. The AUDITQS field is unpredictable when success auditing has not been specified. Use AUDITS instead. Use the AUDITLVL field if you want to permit users to change values on the display panels.

The following table lists the AUDITQS values:

Table 386. AUDITQS values

AUDITQS value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
NONE	FF

AUDITS

This field contains the AUDIT(SUCCESS) level. It is based on the raw AUDIT and AUDITQS fields. The possible values are listed in the following table. The blank (X'FF') value means that success auditing is not active. It is meant for use in SELECT statements. Use the AUDITLVL field for modifiable displays.

AUDITS value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
(blank)	FF

AUTHDATE, CREADATE, DEFDATE

This field is found in all profile types. It indicates the date the profile was created, for example the date the object was defined to RACF.

AUTHOR

This is an alias of OWNER (see “OWNER” on page 1187).

AUTO

This is an alias of AUTOTAPE (see "AUTOTAPEDSN, AUTO").

AUTOTAPE, AUTO

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 1 in the RESFLG field found in TAPEVOL BASE segments. It indicates automatic TAPEVOL profiles. It can be specified as an attribute, SELECT AUTOTAPE for example. Its opposite for the purpose of SELECT/EXCLUDE processing is NOAUTOTAPE. See also the RESFLG field.

BINDDN

This field is found on the PROXY segment of USER and FACILITY class general resource profiles. It specifies the distinguished name (DN) which the z/OS LDAP Server uses when acting as a proxy on behalf of a requester.

BINDPW

This field is found on the PROXY segment of USER and FACILITY class general resource profiles. It contains an LDAP BIND password, and is therefore considered highly confidential. It is not shown on any display or list, and is stored in any unload as *****. It can only be used in SELECT/EXCLUDE processing with the EXISTS or MISSING keyword.

BINDPWKY

This field is found on the PROXY segment of USER and FACILITY class general resource profiles. It contains the encryption method and/or reference to the key of an LDAP BIND password.

CATEGORY

This field is found in USER, DATASET, and GENERAL profiles. For SELECT/EXCLUDE processing, a hexadecimal (internal) value must be specified. It is a repeated field listing the security categories to which the user has access, or to which the data set or resource belongs. The number of security categories is listed in the NUMCTGY field.

CDTINFO segment fields

The following fields provided information about the CDTINFO segment.

CDTCASE, CLASS_CASE_ASIS

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see “CLASS: RACF Class Descriptor Table” on page 989. This field indicates whether profile names in the user-defined class are kept as is or are converted to upper case. The field has a flag format where "Yes" means that the case is preserved, and "No" means that names are converted to uppercase. Use the overriding flag format $CASE to output "UPPER" or "ASIS".

CDTDFTRC, CLASS_DFLTRC

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see “CLASS: RACF Class Descriptor Table” on page 989. This field contains the default return code for the user-defined class. This code is returned when no matching profile can be found in a RACHECK. The return codes and their meaning are documented in the following table.

Table 387. CDTFTRC return codes and descriptions

CDTDFTRC value	Meaning
0	Allow access
4	Indeterminate: depends on resource manager

Table 387. CDTFTRC return codes and descriptions (continued)

CDTDFTRC value	Meaning
8	Fail access

CDTFIRST, CLASS_SYN1RAW

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field contains the syntax rules for the first character of a profile name in the user-defined class. By default this field outputs a four byte character field AN#S. Use overriding format $SYN for command generation. See also CLASS_SYN1ALP, CLASS_SYN1NAT, CLASS_SYN1NUM and CLASS_SYN1SPE.

CDTGEN, CLASS_GENERIC_ALLOWED

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. See "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether SETROPTS GENERIC and SETROPTS GENCMD are authorized for the class. It corresponds to the GENERIC_ALLOWED field in CLASS NEWLIST, see "GENERIC_ALLOWED" on page 997.

CDTGENL, CLASS_GENLIST_ALLOWED

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the user-defined class might be GENLISTed (by using the SETROPTS GENLIST command). Generic profiles for this class are then kept in storage that is shared by all address spaces.

Table 388. CDTGENL values

CDTGENL value	Meaning
Allowed	The GENLIST operation is permitted for this class.
Disallowed	The GENLIST operation is not permitted for this class.

CDTGROUP, CLASS_XGROUP

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. For member classes, this field contains the name of the related grouping class. For non-member classes this field is blank. See also CDTMEMBR.

CDTINFO

This field can only be used for SELECT/EXCLUDE processing. It selects CDTINFO segments.

CDTKEYQL, CLASS_QUAL

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field contains the number of qualifiers at the start of the profile name that cannot be generic. This is a number in the range 0 to 123; the default is 0. During access

verification, RACF ignores all profiles that have generic characters in the specified number of qualifiers. This also controls which profiles are loaded (and kept) in storage.

CDTMAC

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates the way Mandatory Access Control (MAC) uses SECLABELs for the user-defined class. This setting is used only when the SECLABEL class is active. The following table shows the possible values for CDTMAC. See also CLASS_EQUALMAC and CLASS_RVRSMAC.

Table 389. CDTMAC values

CDTMAC value	Meaning
Normal	The SECLABEL of the user must dominate the SECLABEL of the resource to grant access.
Equal	The SECLABEL of the resource and the user must be equivalent
Reverse	The SECLABEL of the resource must dominate SECLABEL of the user to grant access.

CDTMAXLN, CLASS_MAXLEN_ENTITY

Specifies the backward compatible maximum profile name length to be used with the ENTITY keyword form of the RACROUTE macro. The value is a number in the range 1 - 246. The default value is *8*. This field comes from the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. See "CLASS: RACF Class Descriptor Table" on page 989.

This length value is required with the ENTITY keyword form of the RACROUTE macro because that macro form does not pass the return buffer length. As a result, if the maximum profile name length increases, existing applications might break if the entire profile names were returned.

You can avoid this problem by using the ENTITYX keyword form of RACROUTE macro instead. If that form is used, the limit does not apply. See also CDTMAXLX, which contains the true maximum profile name length, if it is different.

CDTMAXLX, CLASS_MAXLEN

Contains the maximum length of resource and profile names for the user-defined class. The value can be a number in the range 1 - 246. By default, the field is missing. This field comes from the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. See "CLASS: RACF Class Descriptor Table" on page 989. See also CDTMAXLN.

CDTMEMBR, CLASS_XMEMBER

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. For grouping classes, this field contains the name of the related member class. For non-grouping classes this field is blank. See also CDTGROUP.

CDTOPER, CLASS_OPER

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether OPERATIONS authority is honored for the user-defined class.

CDTOTHER, CLASS_SYNRRAW

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field contains the syntax rules for the remainder characters of a profile name in the user-defined class. By default this field outputs a four byte character field "AN#S". Use overriding format $SYN for command generation. See also CLASS_SYNRALP, CLASS_SYNRNAT, CLASS_SYNRNUM and CLASS_SYNRSPE.

CDTPOSIT, CLASS_POSIT

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field contains the options set id, a number in the range 0 to 1023 identifying a set of SETROPTS options that govern the activity of the user-defined class and all other classes having the same POSIT value. Whenever a SETROPTS command is issued for any class with a specific POSIT value, it applies to all classes with that same POSIT.

POSIT values in the range 0-18, 57-127, and 528-1023 are reserved for use by IBM; numbers 19-56 and 128-527 are installation-defined.

CDTPRFAL

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether profiles are permitted in the user-defined class.

CDTRACL

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether profiles in the user-defined class might or might not be SETROPTS RACLISTed, or are required to be RACLISTed. If a class is RACLISTed, both generic and discrete profiles for this class are loaded into storage that is shared between all address spaces. Below is a table documenting the different settings. See also CLASS_RACLIST_ALLOWED and CLASS_RACLREQ.

Table 390. CDTRACL values

CDTRACL value	Meaning
Disallowed	The RACLIST operation is not permitted for this class.
Allowed	The RACLIST operation is permitted for this class, but it is not mandatory.
Required	The RACLIST operation is mandatory for this class.

CDTSIGL, CLASS_SIGNAL

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see

"CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether an ENF signal must be sent when the user-defined class is being RACLISTed, NORACLISTed, or RACLIST REFRESHed.

CDTSLREQ, CLASS_SECLABEL

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether security labels are required for resources in the user-defined class. Note that when the SECLABEL class is active, and a security label exists for a resource, the security label for the resource is used during authorization checking, even when security labels are not required.

CDTUACC, CLASS_UACC

Contains the default universal access authority (UACC) for the user-defined class. If no UACC is specified on the command when a profile in this class is added, this default UACC is used to set the profile UACC. The special value ACEE indicates that the UACC is taken from the accessor environment element (ACEE) of the user, which is specified by the UACC on the ADDUSER, ALTUSER or CONNECT command.

This field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. See "CLASS: RACF Class Descriptor Table" on page 989. Table 391 lists the possible UACC values in descending sort order:

Table 391. CDTUACC field - possible UACC values

UACC value	Description
ALTER	• For discrete profiles, ALTER indicates that, by default, all users have control over the resource and the resource profile and can authorize other users or groups (or both) to access the resource. • For generic profiles, ALTER indicates that, by default, all users have control over the resource and can allocate data sets protected by the generic profile. Only the profile owner has full control over the resource profile.
CONTROL	Indicates that, by default, all users have access authority to update, insert, or delete records in the VSAM data set and perform other operations as if the data set password were supplied.
UPDATE	Indicates that, by default, all users can access the resource for both reading and writing.
READ	Indicates that, by default, all users can access the resource for reading only. NONE indicates that, by default, users cannot access the resource.
NONE	Indicates that, by default, users cannot access the resource.
ACEE	Indicates that the UACC is taken from the accessor environment element (ACEE).

CERT and DIGCERT segment fields

The following fields provide information about the CERT and DIGCERT segments.

CERT

Contains the digital certificate in BER-encoded form. This field is only present in profiles in the DIGTCERT class and is part of the CERTDATA segment.

CERTCT

The count of digital certificates associated with this RACF userid or connected to this keyring. This field is only present in the BASE segment of the user profile and the CERTDATA segment of the DIGTRING general resource class. The keys for these certificates are listed in CERTNAME. See also CERTIFICATE_ISSUER and CERTIFICATE_SERIAL.

CERTDATA

Selects CERTDATA segments. This field can only be used for SELECT or EXCLUDE processing.

CERTDFLT

Repeat group field that signifies whether the associated digital certificate is the default certificate for this keyring. The repeat count is stored in the CERTCT field. This field is only present in the CERTDATA segment of the DIGTRING general resource class.

CERTEND

Contains the date and time signifying the end of the validity of this digital certificate. This field is only present in the CERTDATA segment of the DIGTCERT general resource class.

CERTIFICATE_ALT_DOMAIN

Contains the domain names of the subject as found in the subjectAltName extension of the certificate. This field is only present in the CERTDATA segments of profiles in the DIGTCERT class.

CERTIFICATE_ALT_EMAIL

Contains the email addresses of the subject as found in the subjectAltName extension of the certificate. This field is only present in the CERTDATA segments of profiles in the DIGTCERT class.

CERTIFICATE_ALT_IP

Contains the IP address of the subject as found in the subjectAltName extension of the certificate. This field is only present in the CERTDATA segments of profiles in the DIGTCERT class.

CERTIFICATE_ALT_URI

Contains the universal resource identifiers of the subject as found in the subjectAltName extension of the certificate. This field is only present in the CERTDATA segments of profiles in the DIGTCERT class.

CERTIFICATE_ID

Contains the user ID that the digital certificate is related to. This field is only present in the CERTDATA segments of profiles in the DIGTCERT class. When present, the contents of the field is identical to that of the APPLDATA field.

CERTIFICATE_ISSUER

Contains the distinguished name of the issuer of the digital certificate or an approximation of the name. This field is only present for profiles in the DIGTCERT class.

Together with the CERTIFICATE_SERIAL, the CERTIFICATE_ISSUER is a key for the certificate. These fields are derived from the profile KEY, which consists of the serial number and issuer separated by a period. The maximum length for the profile KEY is 246 characters. If the distinguished name for the

certificate issuer is particularly long, the distinguished name portion of the profile key is abbreviated. Abbreviated names are indicated by hash marks in the name portion of the key. If the distinguished name is abbreviated, the value for the CERTIFICATE_ISSUER contains the abbreviated name. The full name can be obtained from the CERTIFICATE_ISSUER_FULL field.

CERTIFICATE_ISSUER_FULL

Contains the full distinguished name of the subject of the certificate issuer. This field is only present in the CERTDATA segment of profiles in the DIGTCERT class. This field is obtained from the certificate, as opposed to CERTIFICATE_ISSUER field which is derived from the profile KEY. See also "CERTIFICATE_ISSUER" on page 1141, "CERT" on page 1140, and CERTIFICATE_SUBJECT.

CERTIFICATE_KEYUSAGE

Contains the keyUsage extension of the certificate. The value can be shown in the KEYUSAGE_RACF format, which is the default RACF format, or it can be shown in the KEYUSAGE_X509 format as defined by the X.509 standard. This field is only present CERTDATA segments of profiles in the DIGTCERT class. See "Specifying syntax for RACF command input" on page 810 for a more detailed description of the formats.

CERTIFICATE_SERIAL

Contains the serial number of the digital certificate. This field is only present for profiles in the DIGTCERT class. Together with the CERTIFICATE_ISSUER field, this is a key for the certificate. These fields are derived from the profile KEY, which consists of the serial number and the issuer separated by a period. See also CERT and CERTIFICATE_ISSUER.

CERTIFICATE_SUBJECT

Contains the distinguished name of the subject of the certificate–the user for whom the certificate was issued. This field is only present for profiles in the DIGTCERT class. This field is interpreted from the actual certificate. See also "CERT" on page 1140 and "CERTIFICATE_ISSUER" on page 1141.

CERTIFICATE_TRUSTED

Flag field that indicates whether the certificate is marked as trusted, and thus whether it is used. This field is only present for profiles in the DIGTCERT class. It is an interpretation of the UACC field.

CERTLABL

Repeat field that contains the list of labels issued to digital certificates associated with the user ID. This field is found in the USER class as part of the BASE segment and in the DIGTRING general resource class as part of the CERTDATA segment. The repeat count is stored in the CERTCT field.

CERTLSER

Contains the last eight bytes of the last certificate that was signed with this key. This field can be found in the CERTDATA segment of the DIGTCERT general resource class.

CERTNAME

Repeat group field that contains a list of digital certificates associated with the user ID or connected to the keyring. This field can be found in the BASE segment of the user profile and the CERTDATA segment of the DIGTRING general

resource class. The repeat count is stored in the CERTCT field. See also CERTIFICATE_ISSUER and CERTIFICATE_SERIAL.

CERTPRVK

Contains the private key for this user, and is therefore considered highly confidential. The value is not shown on any display or list and is stored in any unload file as *****. This field is found on user profiles and is part of the BASE segment. This field can only be used in SELECT or EXCLUDE processing with the EXISTS or MISSING keyword.

CERTPRVS

Contains the size, in bits, of the private key, stored in this digital certificate. This field is only present in the CERTDATA segment of DIGTCERT general resource class profiles.

CERTPRVT

Contains the type of the private key, stored in this digital certificate. This field is only present in the CERTDATA segment of DIGTCERT general resource class profiles.

CERTPUBK

Contains the public key for this user. This field is found on user profiles and is part of the BASE segment.

CERTSEQN

Contains an internal sequence number that is incremented whenever a certificate for the user is added, deleted or altered. This field is found on user profiles and is part of the BASE segment.

CERTSJDN

Repeat group field that contains the list of the distinguished names of the subjects of associated digital certificates. This field can be found in the BASE segment of the user profile and the CERTDATA segment of DIGTRING general resource class profile.The repeat count is stored in CERTCT.

CERTSTRT

Contains the date and time signifying the start of the validity of this digital certificate. This field can be found in the CERTDATA segment of the DIGTCERT general resource class.

CERTUSAG

Repeat group field that contains the list of USAGEs defined for the associated digital certificates within this keyring. Any of the following values can be returned: PERSONAL, SITE, or CERTAUTH. This field can be found in the CERTDATA segment of DIGTRING general resource class profiles. The repeat count is stored in the CERTCT field.

CFDTYPE

This field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field contains the type of data contained by the custom field. Possible values are: *CHAR*, *NUM*, *HEX*, *FLAG*.

CFFIRST

This field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field contains

the syntax rules for the first character of a custom field's value. By default this field outputs a four byte character field AN#S. Use overriding format $CFSYN for command generation. In order to select on CFFIRST, you must use the values from the $CFSYN format. Table 392 shows the possible values of this field.

Table 392. Possible values for CFFIRST and CFOTHER fields

$CFSYN Value	Default output format	Description
ALPHA	AN	Alphabetic and national characters
ALPHANUM	AN#	Alphabetic, national characters, and numerics
ANY	AN#S	All characters
NONATABC	A	Alphabetic only
NONATNUM	A #	Alphabetic and numerics
NUMERIC	#	Numerics only

CFHELP

This field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field contains the help text displayed by TSO when no, or an invalid value has been entered on the ADDUSER, ALTUSER, ADDGRP, or ALTGRP command.

CFLIST

This field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field contains the header text displayed in front of the custom field value in the LISTUSER or LISTGRP command.

CFMIXED

This flag field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field indicates whether the value in a character type custom field keeps its case.

CFMNVAL

This numeric field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field indicates the minimum value of a numeric type custom field.

CFMXLEN

This numeric field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field indicates the maximum length of the custom field's value in number of characters.

CFMXVAL

This numeric field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field indicates the maximum value of a numeric type custom field.

CFOTHER

This field can be found in the CFDEF segment in the CFIELD general resource class. Each profile in this class describes a custom field. This field contains the syntax rules for the remainder characters of a custom field's value. By default

this field outputs a four byte character field AN#S. Use overriding format $CFSYN for command generation. In order to select on CFOTHER you must use the values from the $CFSYN format. Table 392 on page 1144 shows the possible values of this field.

CGAUTHDA, CGCREADT, CGDEFDAT

This repeated field lists the date the user was connected to the group. See the CGGRPCT field.

CGAUTHOR, CGOWNER

This repeated field lists the owner of the connect occurrence, for example the user who created it or last changed it to connect occurrence. See the CGGRPCT field.

CGCREADT

This is an alias of CGAUTHDA field.

CGDEFDAT

This is an alias of CGAUTHDA field. (see "CGAUTH").

CGFLAG1

This repeated field indicates whether the user has the ADSP attribute in the connect group entry. See also the CGGRPCT and GRPADSP fields.

CGFLAG2

This repeated field indicates whether the user has the SPECIAL attribute in the connect group entry. See also the CGGRPCT and GRPSPEC fields.

CGFLAG3

This repeated field indicates whether the user has the OPERATIONS attribute in the connect group entry. See also the CGGRPCT and GRPOPER fields.

CGFLAG4

This repeated field indicates whether the user has the REVOKE attribute in the connect group entry. See also the CGGRPCT and GRPREVOKE fields.

CGFLAG5

This repeated field indicates whether the user has the GRPACC attribute in the connect group entry. See also the CGGRPCT and GRPGRPACC fields.

CGGRPAUD

This repeated field indicates whether the user has the group-AUDITOR attribute within the connect group entry. See also the CGGRPCT and GRPAUD fields.

CGGRPCT

This field lists the number of connect group entries. It is only found in user profiles. The connect fields are CGGRPNM, CGAUTHDA, CGAUTHOR, CGLJTIME, CGLJDATE, CGUACC, CGINITCT, CGFLAG1, CGFLAG2, CGFLAG3, CGFLAG4, CGFLAG5, CGNOTUAC, CGGRPAUD, CGREVKDT, and CGRESMDT.

CGGRPNM

This repeated field lists the connect group entry names, in alphabetical order. See the CGGRPCT field.

CGINITCT

This repeated field lists the number of RACINITs issued for the connect group entry. This field is only updated if RACINIT statistics are on (due to SETROPTS INITSTATS). See the CGGRPCT field.

CGLJDATE

This repeated field lists the last RACINIT date for the connect group entry. This field is only updated if RACINIT statistics are on (due to SETROPTS INITSTATS). See the CGGRPCT field.

CGLJTIME

This repeated field is only found in user profiles. It lists the last RACINIT time for the connect group entry and can only be used for output. This field is only updated if RACINIT statistics are on (due to SETROPTS INITSTATS). See also the CGGRPCT and CGLJDATE fields.

CGNOTUAC

This repeated field indicates whether the user is authorized to use a terminal not defined to RACF for the connect group entry. See the CGGRPCT field.

CGOWNER

This is an alias of CGAUTHOR field. (see "CGAUTHOR" on page 1145).

CGRESMDT

This repeated field lists the resume date for the connect group entry. See the CGGRPCT field.

CGREVKDT

This repeated field lists the revoke date for the connect group entry. See the CGGRPCT field.

CGUACC

This repeated field lists the universal access for the connect group entry. See the CGGRPCT field for connect information; see the GRPADSP field for the meaning of the CGUACC field.

CHILDN

This field is found in the ROLE class and is part of the TME segment. It is the count of child roles of the role. These child roles are listed in CHILDREN.

CHILDREN

This field is found in the ROLE class as part of the TME segment. It is a repeat group field; the repeat count is stored in the CHILDN field. It contains the list of child roles of the role.

CHECKADDRS, CHKADDRS

This flag field is found in the KERB segment of RACF profiles in the REALM class. The field specifies whether the Kerberos server validates network addresses in encrypted tickets as part of ticket validation processing. The flag is used for the KERBDFLT profile only; this profile is created in the REALM class and defines the local realm.

CICS

This field can only be used for SELECT/EXCLUDE processing. It selects CICS segments.

CICS_RSLKEY

This pseudofield contains all the values of the repeated field RSLKEY, and is, like its source field, present in the CICS segment of user profiles. It is meant for easy administration of the Resource Security Level Keys assigned. It can also be printed with the overriding format SLKEY_COMPACT, which shows all Security Level Keys in ranges (*10:25*, for example).

CICS_TSLKEY

This pseudofield contains all the values of the repeated field TSLKEY, and is, like its source field, present in the CICS segment of user profiles. It is meant for easy administration of the Transaction Security Level Keys assigned. It can also be printed with the overriding format SLKEY_COMPACT, which show all Security Level Keys in ranges (*10:25* for example).

CKGAUTH

Variable defined in C2RXDEF1 that contains the CKGRACF authority requirement (`SINGLE`, `DUAL`, or `TRIPLE`) of a profile, if set.

CKGAUTHOR

This field is derived from the USR field and contains the `userid` of the user who requested a CKGRACF queued command. It is repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.

CKGCHGDATE

This field is derived from the USR field and contains the date a queued command was last changed. It is repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.

CKGEVENTS

Variable defined in C2RXDEF1 that contains the CKGRACF schedules for a profile.

CKGEXPIRY

This field is derived from the USR field and contains the first date on which any of the queued commands expires. Each queued command has one expiration date. This field shows the value of the earliest expiration date in the queue. Undefined if the profile does not contain queued commands.

CKGMULTI

This field is derived from the USR field and contains the multiple-authority setting; can be SINGLE, DUAL, or TRIPLE if set; otherwise undefined.

CKGOTHER

Variable defined in C2RXDEF1 that contains the `CKGRACF` entries that are not contained in `CKGAUTH` (authority requirement), `CKGEVENTS` (schedules), `CMDSEXEC`, `CMDSINACT`, and `CMDSPEND` (executed, rejected, and pending queued commands). Together these are the complement of `USERDATA` (non-CKGRACF entries) with respect to `USR` (all user data entries).

CKGREFRESH

This field is derived from the USR field and contains the date after which a CKGRACF REFRESH command is required; undefined if the profile does not contain scheduled revoke/resume actions or queued commands.

CKGREQUEST

This field is derived from the USR field and contains the date a queued command was requested. The value is repeated for each queued command stored in the profile. If the profile does not contain queued commands, the value is undefined.

CKGSCHEDULE, CKGSCHED

This field is derived from the USR field and contains the schedule name of a scheduled revoke/resume action. It is repeated for each scheduled action stored in the profile; undefined if the profile does not contain scheduled actions.

CKGSTATUS

This field is derived from the USR field and contains the current status of a queued command. It is repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands. The values are listed in the following table. (The abbreviations used to indicate this status in the output of the USR field.)

Table 393. CKGSTATUS values for queued commands

Value	USR abbreviation
COMPLETE APPROVE	(CA)
COMPLETE DENY	(CD)
COMPLETE HOLD	(CH)
EXPIRE	(E)
PENDING	(P)
PENDING REVERSE	(PR)
REQUEST	(R)
SECOND APPROVE	(SA)
SECOND DENY	(SD)
SECOND HOLD	(SH)
WITHDRAW	(W)
EXECUTED	(X)

CLASS, C

Provides the RACF class, USER, GROUP, DATASET, PROGRAM, ACCTNUM, or GCICSTRN, for example.

When used for SELECT/EXCLUDE processing, the special value GENERAL indicates all kinds of general resource classes. If used in combination with the MATCH or BESTMATCH keyword, the class selection has a special meaning, selecting both a member class and its grouping class.

CLASTYPE

This field is only found in GENERAL profiles. It lists the class number from the Class Descriptor Table (CDT, see the ID field of NEWLIST TYPE=CLASS). This number indicates the class to which the profile belongs, but it is not used by RACF.

CLASS_CASE_ASIS

This is an alias of CDTCASE.

CLASS_DFLTRC

This is an alias of CDTDFTRC.

CLASS_EQUALMAC

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether equal mandatory access checking is performed for resources in this user-defined class. This means that in order to be granted access to a resource, the SECLABEL of the user and the resource must be equivalent (have the same security level and categories). This setting is used only when the SECLABEL class is active. See also CLASS_RVRSMAC and the combination field CDTMAC. The value in this field cannot be changed on an ISPF panel. If you want to permit users to change the value, use the CDTMAC field.

CLASS_GENLIST_ALLOWED

This is an alias of CDTGENL.

CLASS_MAXLEN

This is an alias of CDTMAXLX.

CLASS_MAXLEN_ENTITY

This is an alias of CDTMAXLN.

CLASS_OPER

This is an alias of CDTOPER.

CLASS_POSIT

This is an alias of CDTPOSIT.

CLASS_QUAL

This is an alias of CDTKEYQL.

CLASS_RACLIST_ALLOWED

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the user-defined class might be RACLISTed by issuing the SETROPTS RACLIST command. When a class is RACLISTed, both discrete and generic profiles are loaded into storage that is shared between all address spaces. See also CLASS_RACLREQ, and the combination field CDTRACL. The value in this field cannot be modified from an ISPF panel. If you want to permit users to change the value, use the CDTRACL field.

CLASS_RACLREQ

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the user-defined class must be RACLISTed. When a class is RACLISTed, both generic and discrete profiles are loaded into storage that is shared between all address spaces. See also CLASS_RACLIST_ALLOWED, and the combination field CDTRACL CDTRACL.

CLASS_RVRSMAC

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether reverse mandatory access checking is performed for resources in the

user-defined class. This means that the SECLABEL of the resource must dominate the SECLABEL of the user. This setting is used only when the SECLABEL class is active. See also CLASS_EQUALMAC, and the combination field CDTMAC. The value in this field cannot be modified from an ISPF panel. If you want to permit users to change the value, use the CDTMAC field.

CLASS_SECLABEL

This is an alias of CDTSLREQ.

CLASS_SIGNAL

This is an alias of CDTSIGL.

CLASS_SYN1ALP

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the first character of a profile in the user-defined class might be alphabetical. Combine this flag with the CLASS_SYN1NAT, CLASS_SYN1NUM, and CLASS_SYN1SPE flags to determine all legal first characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTFIRST.

CLASS_SYN1NAT

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the first character of a profile in the user-defined class might be a national character (#, @, and $). Combine this flag with the CLASS_SYN1ALP, CLASS_SYN1NUM, and CLASS_SYN1SPE flags to determine all legal first characters. This value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the CDTFIRST field. CDTRACL

CLASS_SYN1NUM

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the first character of a profile in the user-defined class can be a numeric character. Combine this flag with the CLASS_SYN1ALP, CLASS_SYN1NAT, and CLASS_SYN1SPE flags to determine all legal first characters. See also the combination field CDTFIRST. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination CDTFIRST field.

CLASS_SYN1RAW

This is an alias of CDTFIRST.

CLASS_SYN1SPE

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether the first character of a profile in the user-defined class can be a special character (any character other than alphabetical, numerical, national, blank, comma, parenthesis or semicolon). Combine this flag with the CLASS_SYN1ALP, CLASS_SYN1NAT, and CLASS_SYN1NUM flags to

determine all legal first characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTFIRST.

CLASS_SYNRALP

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether all characters other than the first character of a profile in the user-defined class can be alphabetical. Combine this flag with the CLASS_SYNRNAT, CLASS_SYNRNUM, and CLASS_SYNRSPE flags to determine all legal remainder characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTOTHER.

CLASS_SYNRNAT

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class; see "CLASS: RACF Class Descriptor Table" on page 989. This field indicates whether all characters other than the first character of a profile in the user-defined class can be a national character (#, @, and $). Combine this flag with the CLASS_SYNRALP, CLASS_SYNRNUM, and CLASS_SYNRSPE flags to determine all legal remainder characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTOTHER.

CLASS_SYNRNUM

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. This field indicates whether all characters other than the first character of a profile in the user-defined class can be a numeric character (0-9). Combine this flag with the CLASS_SYNRALP, CLASS_SYNRNAT, and CLASS_SYNRSPE flags to determine all legal remainder characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTOTHER.

CLASS_SYNRRAW

This is an alias of CDTOTHER.

CLASS_SYNRSPE

This flag field can be found in the CDTINFO segment in the CDT general resource class. Each profile in this class describes a user-defined class. This field indicates whether all characters other than the first character of a profile in the user-defined class can be a special character (any character other than alphabetical, numerical, national, blank, comma, parenthesis, or semicolon). Combine this flag with the CLASS_SYNRALP, CLASS_SYNRNAT, and CLASS_SYNRNUM flags to determine all legal remainder characters. The value in this field cannot be changed from an ISPF panel. If you want to permit users to change the value, use the combination field CDTOTHER.

CLASS_UACC

This is an alias of CDTUACC.

CLASS_XGROUP

This is an alias of CDTGROUP.

CLASS_XMEMBER

This is an alias of CDTMEMBR.

CLCNT

This field indicates the number of classes for which the user has the CLAUTH attribute. It is only found in user profiles. The CLNAME field lists the classes.

CLNAME

Repeated field that lists the classes in which the user is permitted to define profiles. That is classes for which the user has the CLAUTH attribute. This field is only found in user profiles. Each entry is 8 characters. The CLCNT field lists the number of classes.

CMDSEXEC

Variable defined in C2RXDEF1 that contains the CKGRACF queued commands that have been performed. They are kept according to the CKGRACF audit period. See also CMDSINACT and CMDSPEND.

CMDSINACT

Variable defined in C2RXDEF1 that contains the CKGRACF queued command requests that have been rejected. These commands were withdrawn, have expired, or were denied by a responsible administrator. They are kept according to the CKGRACF audit period. See also CMDSEXEC.

CMDSPEND

Variable defined in C2RXDEF1 that contains commands pending in the CKGRACF execution queue, both Pending (P) and Pending Reverse (PR). See also CMDSEXEC and CMDSINACT.

CNGAUTH

Variable defined in C2RXDEF1 that is equivalent to CKGAUTH.

CNGAUTHOR

This is an alias of CKGAUTHOR.

CNGCHGDATE

This is an alias of CKGCHGDATE.

CNGEVENTS

Variable defined in C2RXDEF1 that is equivalent to CKGEVENTS.

CNGEXPIRY

This is an alias of CKGEXPIRY.

CNGMULTI

This is an alias of CKGMULTI.

CNGOTHER

Variable defined in C2RXDEF1 that is equivalent to CKGOTHER.

CNGREFRESH

This is an alias of CKGREFRESH.

CNGREQUEST

This is an alias of CKGREQUEST.

CNGSCHEDULE, CNGSCHED

This is an alias of CKGSCHEDULE.

CNGSTATUS

This is an alias of CKGSTATUS.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

CONCERN

This is an alias of the AUDITCONCERN field.

CONGRPCT

This field indicates the number of groups to which the user is connected. It is only found in user profiles. The CONGRPNM field lists the groups.

CONGRPNM

This is a repeated field listing the groups to which the user is connected, in chronological order (for example, in the order in which the user was connected to each group). This field is only found in user profiles. The CONGRPCT field lists the number of groups.

Note: This field should *not* be combined with the CG... fields for listing group occurrences. All CG... fields are sorted in alphabetical order, and the CONGRPNM field is sorted in chronological order. Use the CGGRPNM field instead.

CONNECT

This field shows an integrated display of the connect attributes Authority, Revoke status, Special, Operations, Audit, ADSP, Group-access, UACC, Revoke date, and Resume date. It can only be used for output on the DISPLAY, SORTLIST, and (D)SUMMARY commands. It must be specified based on an indirect reference to USERID when displaying a group profile, and based on an indirect reference to CONGRPNM or CGGRPNM when displaying a user profile. This field combines information from group profiles with information from user profiles, and interprets the revoke/resume dates and flag against the date of RACF unload (or the current date, if not unloaded). When running on z/OS 1.7 or higher, revoke/resume dates are always shown, if present. In earlier releases, these dates were only shown for future dates. Be aware that connect information is needed, so displaying this field works best if specified in the scope of a NEWLIST while there are no outer selections.

CONNECT_COUNT

This pseudo-field is only found in GROUP BASE segments and contains the number of users connected to the group. Unlike the ACLCNT field it shows the total count of all connected users even for UNIVERSAL groups. This value can only be calculated when a full database read has been done. To force a full database read when not using an UNLOAD you can specify the UNIVERSAL

modifier on this field. This field can only be used on the SORTLIST, DISPLAY and (D)SUMMARY commands, and not on SELECT and EXCLUDE.

CONNECTS

Shows an integrated display with the following information about connect attributes: authority level, Revoke status, Special, Operations, and Auditor attributes, ADSP value, Group-access and UACC list, Revoke date, and Resume date. The value in the revoke date field can be modified by typing a date (*ddmmmyyyy*) or removed by typing the text *NOREVOKE*. The value in the Resume date field can be modified by typing a date (*ddmmmyyyy*) or removed by typing the text *NORESUME* .

For user profiles, it shows connected groups and the connect attributes; for group profiles, it shows connected users and connect attributes. If no connect authority is specified on the group profile, a value of USE is assumed. This field combines information from group profiles with information from user profiles, and interprets the revoke/resume dates and flag against the date of the RACF unload (or the current date, if not unloaded). For z/OS 1.7 and later, revoke/resume dates are always shown, if present. In earlier releases, these dates were only shown when if they were future dates. Be aware that connect information is needed, so displaying this field works best if specified in the scope of a NEWLIST while there are no outer selections, or with the UNIVERSAL modifier specified to force collection of all relevant data.

The DEFINE SUBSELECT command can be used to select specific repeat group instances for output, only group-SPECIAL connects for example. See "Subselect clauses" on page 755.

To print just the ids, use overriding length 8. To print only specific connect attributes, use a lookup, e.g. CONNECTS:GRPSPEC.

CONSNAME

This field is found in user profiles and is part of the NETVIEW segment. It contains the default MCS console identifier.

CONVSEC

This field is found on the SESSION segment of the APPCLU general resource profile. It specifies the level of security checking performed when conversations are established with the LU protected by this profile.

CPUTIMEMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum CPU time that a process can use, in seconds. It lies between 7 and 2,147,483,647.

CREADATE

This is an alias of AUTHDATE field. (see "AUTHDATE" on page 1135).

CSCNT

This field can be found in the CSDATA segment of user and group profiles. It lists the number of custom field entries. The preferred interface to this field is the CUSTOM_DATA field.

CSFAUSE, ASYMUSAGE

Specifies how an asymmetric key controlled can be used by the general resources profiles in the following classes CSFKEYS, GCSFKEYS, XCSFKEY,and

GXCSFKEY. The field can be found in the ICSF segment that specifies attributes for the keys controlled by these profiles. Table 394 shows the possible field values.

Table 394. ASYMUSAGE field values for use of asymmetric key

ASYMUSAGE value	Default output format	Description
SECUREEXPORT HANDSHAKE	SH	The asymmetric key can be used to import or export symmetric keys (SECUREEXPORT) and to protect communication channels (HANDSHAKE). This is the default value.
NOSECUREEXPORT HANDSHAKE	H	The asymmetric key can only be used to protect communication channels (HANDSHAKE).
SECUREEXPORT NOHANDSHAKE	S	The asymmetric key can only be used to import or export symmetric keys (SECUREEXPORT).
NOSECUREEXPORT NOHANDSHAKE	blank	The asymmetric key cannot be used to import or export symmetric keys (NOSECUREEXPORT) nor to protect communication channels (NOHANDSHAKE) .

Asymmetric key usage values for selection can be (NO)SECUREEXPORT, (NO)HANDSHAKE, or a combination of values as shown in Table 394. You can only modify the CFSAUSE, ASYMUSAGE field indirectly using the HANDSHAKE and SECUREEXPORT fields. You can use overriding format `$AsymKeyUsage` for command generation. (See "Specifying syntax for RACF command input" on page 810.)

CSFSCPW, SYMCPACFWRAP

Indicates if the symmetric keys covered by this profile can be rewrapped. This value comes from the ICSF segment which specifies attributes for the keys controlled by general resources profiles in the `CSFKEYS, GCSFKEYS`.

CSFSEXP, SYMEXPORTABLE

Indicates whether the symmetric keys covered by this profile can be exported. This value comes from the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY. Table 395 shows the possible values of this field.

Table 395. SYMEXPORTABLE field values

SYMEXPORTABLE value	Default output format	Description
BYANY	ANY	The symmetric key can be exported without restriction. The SYMEXPORTCERTS and SYMEXPORTKEYS fields are ignored; this is the default.
BYLIST	LIST	The symmetric key can only be exported by a public key which is identified in the SYMEXPORTCERTS or SYMEXPORTKEYS field. If neither field exists, then the key cannot be exported. This is equivalent to the BYNONE option.
BYNONE	NONE	The symmetric key cannot be exported. The SYMEXPORTCERTS and SYMEXPORTKEYS fields are ignored.

Symmetric key exportable values for selection can be (BY)ANY, (BY)LIST, or (BY)NONE. You can use overriding format $SymKeyExp for command generation.

CSFSCLBS, SYMEXPORTCERTS

This repeat group field can be found in the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY. In particular, this field specifies a list of digital certificate labels that can be used to export the symmetric keys controlled by these profiles. The certificate must exist within the SAF key ring or PKCS#11 token identified in an ICSF configuration setting. Its default output length is 73 characters. This field can be modified. See *Cryptographic Services ICSF Administrator's Guide* for more information.

CSFSCLCT

This field can be found in the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY. In particular, this field denotes the number of certificate labels that can be used to export the symmetric keys controlled by these profiles. See also the CSFSCLBS field.

CSFSKLBS, SYMEXPORTKEYS

This repeat group field can be found in the ICSF segment that specifies attributes for the keys controlled by general resource profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY. This field specifies a complete list of the ICSF key labels pertaining to public keys that can be used to export the symmetric keys covered by these profiles. The label name must not exceed 64 characters, which in effect is its default output length. The first character must be alphabetic or national (@, #, and $). Subsequent characters can be alphanumeric (including the national characters) or a period. This field can be modified. See *Cryptographic Services ICSF Administrator's Guide* for more information.

CSFSKLCT

This field can be found in the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY. In particular, this field denotes the number of PKDS labels which can be used to export the symmetric keys covered by these profiles. See "CSFSKLBS" for more information.

CSKEY

This repeated field can be found in the CSDATA segment of user and group profiles. Each entry contains a custom field's name. The preferred interface for reporting this information is the CUSTOM_DATA field, or use the content of CSKEY directly as a field name.

CSTYPE

This repeated field can be found in the CSDATA segment of user and group profiles. Each entry contains a custom field's type.

CSVALUE

This repeated field can be found in the CSDATA segment of user and group profiles. Each entry contains a custom field's value. The preferred interface to this field is to use the CSKEY content as a field name directly or use the CUSTOM_DATA field.

CTL

This field is found in user profiles and is part of the NETVIEW segment. It contains a flag that specifies whether a security check should be performed for this NetView operator for a span or a cross-domain logon. This field can have the values **General**, **Global**, and **Specific**.

CURKEY

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the current key for the user or realm in encrypted form. This field is removed from any UNLOAD made.

CURKEYV

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the version number of the current key for the user or realm.

CUSTOM_DATA

Repeated field that contains the custom list header for the field followed by the value of the field. This field can be found in the CSDATA segment of user and group profiles. The field can only be specified on the following commands: DISPLAY, DSUMMARY, SORT, SORTLIST, and SUMMARY.

You can use the DEFINE SUBSELECT command to display only selected repeat group entries. See "Subselect clauses" on page 755. You can use the SELECT CUSTOM_DATA(...) command to select on specific combinations of values per repeat group entry. See "SELECT/EXCLUDE CUSTOM_DATA(...)" on page 890.

To only print the value of the CUSTOM_DATA field, use the CSVALUE format. To print the name of the field followed by its value in parenthesis, use the $CUSTOM_DATA format. This latter format can be used for command generation.Beginning with zSecure V1R11, the output for the CUSTOM_DATA field can only be formatted using the WRAP format field if the MODIFIABLE attribute for the CUSTOM_DATA field is turned off. The WRAP and MODIFIABLE options can be specified using the FIELD NEWLIST. See "FIELD: Field Properties per NEWLIST type" on page 1034. If the WRAP modifier is specified for a new field, the MODIFIABLE attribute is automatically turned off.

DATA

This is an alias of INSTDATA (see "INSTDATA, DATA" on page 1172).

DATAAPPL

For user or group profiles, this field provides the DPF-data application in DFP segment.

DATACLAS

For user or group profiles, this field provides DFP-data class in the DFP segment.

DB

This field contains the three-digit sequence number of the data set in the RACF database originally containing the profile. The data sets making up the RACF databases, their sequence numbers, and the profile key ranges can be displayed using the NEWLIST TYPE=RRNG.

DCE

This field can only be used for SELECT or EXCLUDE processing. It selects DCE segments.

DCEENCRY

This field is found in the DCE segment of the user profile. It contains the DCE password mask/encrypt key.

DCEFLAGS

This field is found on the DCE segment of the user profile. It specifies whether z/OS UNIX DCE automatically attempts to sign on this user to z/OS UNIX DCE.

DCENAME

This field is found on the DCE segment of the user profile. It contains the DCE principal name of this user.

DEFDATE

This is an alias of AUTHDATE (see "AUTHDATE" on page 1135).

DEFTKTLF

This field can be found in the KERB segment for the REALM General Resource class. It contains the default ticket life in seconds that is granted when generating a ticket for the target system.

DEPTH

This field can only be used for output processing, on a SORTLIST, DISPLAY or (D)SUMMARY command. It is defined for group profiles and indicates the depth of the group within the group tree. It is mainly of use to sort commands that apply to several groups in succession, or as INDENT parameter in a group-tree display.

DEVTYP

This field is found in DATASET profiles. It indicates the device type on which the data set resides. Not specified for generic profiles and some non-VSAM discrete profile types. The default output format is a hexadecimal representation of a unit type.

DEVTYPX, UNIT

This text field is found in DATASET profiles. It contains the name of the device type on which the data set resides. Not specified for generic profiles and some non-VSAM discrete profile types.

The UNIT field name can only be used for SELECT/EXCLUDE processing.

DFLTGRP

The default connect group of a user. This field is only found in user profiles.

DFP

This field can only be used for SELECT/EXCLUDE processing. It selects DFP segments.

DIDCT

This field is found in IDIDMAP profiles. It contains the number of identity mappings in the profile. The distributed identity given by each DIDRNAME

11. For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

(registry) and the KEY (identity filter, which can be in X.500 format) is mapped to the RACF userid in each corresponding DIDUSER. See the DIDUSER the field.

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DIDLABL

This repeat group field is found in IDIDMAP profiles. It contains the labels for the identity mappings. The repeat count is contained in the field DIDCT. See the DDIDCT and the DMAPLABL.

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DIDRNAME

This repeat group field is found in IDIDMAP profiles. It contains the registries for the distributed identities mapped. The repeat count is contained in the field DIDCT. Also, see the RACMAP_REGISTRY and IDIDMAP_CMD_REGISTRY fields.

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DIDUSER

This repeat group field is found in IDIDMAP profiles. It contains the RACF userids to which the distributed identities are mapped. The repeat count is contained in the field DIDCT. (See "DIDCT" on page 1158.)

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DIGTCERT_LABEL

This field is only present for digital certificates (for example, profiles in the DIGTCERT class). It contains the certificate label of the certificate and corresponds to the CERTLABL field in USER, DIGTRING and DIGTNMAP profiles. It can be used as an alternative key for most RACDCERT commands. This field cannot be used for SELECT/EXCLUDE processing.

DIGTRING_USERID

For a profile in the DIGTRING class, this field contains the userid the keyring is related to; for other classes it is absent. When present the content of the field is identical to that of the APPLDATA field.

DISCRETE

This field can only be used for SELECT/EXCLUDE processing. It is used to select discrete DATASET and GENERAL profiles. It can be specified as an attribute, for example SELECT DISCRETE. Use the PROFTYPE output field to display the profile type.

DLFDATA

This field can only be used for SELECT/EXCLUDE processing. It selects DLFDATA segments.

DMAPCT

This field is found in the BASE segment of user profiles. It contains the number of identity mappings that map to the RACF userid. The distributed identities are given by each RACMAP_REGISTRY (registry) and DMAPNAME (identity filter, which can be in X.500 format).

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DMAPLABL

This repeat group field is found in the BASE segment of user profiles. It contains the identity filter (which can be in X.500 format) for the identity mappings to this userid. Together with the userid, the label uniquely identifies a particular identity mapping. The repeat count is contained in the DMAPCT field.

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DMAPNAME

This repeat group field is found in the BASE segment of user profiles. It contains the identity filter (which can be in X.500 format) for the identity mappings to this userid. The repeat count is contained in the field DMAPCT. See "DMAPCT" on page 1159 and "RACMAP_CMD_FILTER" on page 1193.)

For additional information on distributed identity filters, distributed identity mapping, and IDIDMAP profiles, see the *Security Server RACF Security Administrator's Guide* for z/OS Version 1 Release 11 or later.

DOMAINDN

This field is found on the EIM segment of LDAPBIND and FACILITY class general resource profiles. It specifies the distinguished name of the EIM domain. This field supports the overtype which permits authorized users to change the field value from an ISPF panel.

DOMAINS

This field is found in user profiles and is part of the NETVIEW segment. It is a repeated field; the repeat count is stored in the DOMAINSN field. Each repeat group entry contains the name of a Netview program in another domain; the operator has authority over the Netview programs listed by this field.

DOMAINSN

This field is found in user profiles and is part of the NETVIEW segment. It contains the repeat count for the DOMAINS field.

DOMAP

This field is found in the ICTX segment of IRR.ICTX.DEFAULTS.** profiles in the LDAPBIND general resource class. It specifies whether the Identity Context Extension (ICTX) uses Enterprise Identity Mapping (EIM) services to find a mapping to a z/OS user ID. This field supports the overtype option which permits authorized users to change the value from an ISPF panel.

DPASSWDS

This field is found on the DCE segment of the user profile. It contains the current DCE password.

DSN

This field is equivalent to the KEY and PROFILE fields, but it is only defined for data set profiles. It contains the name of a data set profile.

DSTYPE

This field is found in DATASET BASE segments, and can only be used for output. The following table lists the DSTYPE values and their meaning:

Table 396. DSTYPE values

DSTYPE value	Meaning
MODEL	Model profile
TAPE	Tape data set
VSAM	VSAM
(blank)	None of the above

For SELECT/EXCLUDE processing, use the MODEL, TAPE, and VSAM fields.

EIM

This field can only be used for SELECT/EXCLUDE processing. It selects EIM segments.

ENCRYPT

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the encryption types that can be used when establishing a connection.

ENCTYPE

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the encryption type that has been used to establish a connection.

ENTITY

This field is similar to CLASS, but it returns GENERAL for all general resource classes. Meant for use like SUMMARY ENTITY SEGMENT.

ENTYPE

This field can be found in all profile types and indicates the profile entity type. It is a numerical value of up to three digits. The following table lists the entity types defined.

Table 397. Entity type definitions

ENTYPE value	Profile type
1	GROUP
2	USER
3	CONNECT
4	DATASET
5	GENERAL

ERASE

This field is only found in DATASET BASE segments. It indicates whether the erase-on-scratch flag is set. It can be specified as an attribute, e.g., .SELECT ERASE. Its opposite for the purpose of SELECT/EXCLUDE processing is NOERASE.

Note that a data set profile's erase-on-scratch setting is only honored if erase-on-scratch is in effect (due to SETROPTS ERASE). This is indicated by the ERASEONSCRATCH field of NEWLIST TYPE=SYSTEM.

FAILLOAD

FAILLOAD is found in GENERAL resource profiles and is part of the SIGVER segment.

The value in this field indicates what action the system loader is to take when signature verification fails. This field can be based on the value of the field or the presence of the field. The following values can be displayed. The field can be selected based on the value in the field or the presence of the field.

Table 398. Fail reasons

Value	Description
ANYBAD	Specifies that the program fails to load when a signature verification failure occurs, regardless of the cause.
BADSIGONLY	Specifies that the program fails to load only when the signature verification failure is caused by an incorrect digital signature.
NEVER	Specifies that the program never fails to load because a signature verification failure is detected.

FILEPROCMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum number of files that this user is permitted to have open at any given time. It lies between 3 and 262,143 (pre-z/OS V1R7) or 524,288 (z/OS V1R7 and up).

FILTER, MASK

This field can only be used for SELECT/EXCLUDE processing. It is used to search for the profile key using a pattern match. For example, FILTER=SYS1.** matches all profile keys that start with SYS1. To search for an exact profile key, use the KEY field instead. To search for all profiles that could match a given resource name, use the MATCH field instead.

A mask for the profile key. Use %, *, and .** (enhanced generic naming). The filter is *always* interpreted as enhanced generic, independent of the RACF database setting for EGN. If you specify a generic profile key here, this matches generic profiles and discretes that are covered by this name.

The meaning of a single * depends on the entity type. For data sets only, it matches a qualifier with a maximum of 8 characters. Note that for general resource profiles, the * at the end of FILTER selects only a single qualifier (while in RACF it means any number of qualifiers).

FILTER_ISSUERDN

This pseudofield exists only for profiles in the DIGTNMAP class and contains the description for the filter of the issuer's distinguished name. See also FILTER_SUBJECTDN and FLTRNAME.

FILTERCT

This pseudofield exists only for profiles in the DIGTNMAP class and contains the description for the filter of the subject's distinguished name. See also FILTER_ISSUERDN and FLTRNAME.

FILTERCT

This field can be found in the BASE segment of a general resource profile in the DIGTNMAP class. It is the count of digital certificate filters that map to the key of this profile.

FLAG1

For user profiles, this flag byte field indicates the ADSP attribute. See the ADSP field. For DATASET profiles, this flag indicates a group data set. See the GROUPDSN field.

FLAG2

For user profiles, this flag byte field indicates the SPECIAL attribute. See the SPECIAL field.

FLAG3

For user profiles, flag byte field that indicates the OPERATIONS attribute. See the OPER field.

FLAG4

For user profiles, flag byte field that indicates the REVOKE attribute. See the REVOKE field.

FLAG5

For user profiles, flag byte field that indicates the GRPACC attribute. See the GRPACC field.

FLAG6

For user profiles, flag byte field that indicates the AUDITOR attribute, see the AUDITOR field.

FLAG7

This flag field is found in the BASE segment of user profiles. It contains password, protected and password phrase flag bits. By default, this flag byte is printed hexadecimal. See also fields HAS_PASSWORD, PROTECTED, and HAS_PHRASE.

FLAG8

For user profiles, this flag byte field indicates if the user requires an OID card to logon. See the OIDCARD field.

FLAG9

For user profiles, this flag byte field indicates if the user has the RESTRICTED attribute, see the RESTRICTED field.

FLAGPRIV

This field is found in STARTED profiles and is part of the STDATA segment. It indicates whether a started procedure matching the profile should run privileged (FLAGPRIV=YES) or not (FLAGPRIV=NO). If the FLAGPRIV field is set to YES, indicating the started procedure should run privileged, the FLAGTRUS flag is ignored.

FLAGTRAC

This field is found in STARTED profiles and is part of the STDATA segment. It indicates whether a started procedure matching the profile should be traced

(FLAGTRAC=YES) or not (FLAGTRAC=NO). If the started procedure is traced, RACF issues message IRR812I to indicate the profile and started procedure used.

FLAGTRUS

This field is found in STARTED profiles and is part of the STDATA segment. It indicates whether a started procedure matching the profile should run trusted (FLAGTRUS=YES) or not (FLAGTRUS=NO). If the FLAGPRIV field is set to YES, indicating the started procedure should run privileged, the FLAGTRUS flag is ignored.

FLDCNT

For all profile types: field counting the number of FLDNAME, FLDVALUE and FLDFLAG fields.

FLDFLAG

For all profile types: reserved field. This repeated field can be combined with the FLDVALUE and FLDNAME fields. The count is listed in the FLDCNT field.

This field indicates the erase-on-scratch flag for DATASET profiles, if the corresponding FLDNAME field is set to EOSFLAG.

FLDNAME

For all profile types: reserved field. This repeated field can be combined with the FLDVALUE and FLDFLAG fields. The count is listed in the FLDCNT field.

For DATASET profiles: If this field is set to EOSFLAG, then FLDFLAG is the erase-on-scratch flag. This setting is easier to display with the ERASE field.

FLDVALUE

For all profile types: reserved field. This repeated field can be combined with the FLDNAME and FLDFLAG fields. The count is listed in the FLDCNT field.

FLTRLABL

This field is found in the BASE segment of a general resource profile in the DIGTNMAP class. It is a repeat group field; its count is stored in the FILTERCT field. It shows the list of labels describing the digital certificate filters that map to the key of this profile.

FLTRNAME

This field is found in the BASE segment of a general resource profile in the DIGTNMAP class. It is a repeat group field; its count is stored in the FILTERCT field. It contains a list of descriptions of the digital certificate filters that map to the key of this profile. This description contains a filter for the issuer's distinguished name and one for the subject's distinguished name, separated by a ¢. See also FILTER_ISSUERDN and FILTER_SUBJECTDN.

FLTRSTAT

This field is found in the BASE segment of a general resource profile in the DIGTNMAP class. It is a repeat group field; its count is stored in the FILTERCT field. It contains the status of the digital certificate filters that map to the key of this profile, for example whether they are TRUST or NOTRUST.

FLTRUSER

This field is found in the BASE segment of a general resource profile in the DIGTNMAP class. It is a repeat group field that contains a list of the user IDs specifying the RACF user ID that the digital certificate filters described in this

profile map to. This field can also contain the generic key description for a profile in the DIGTCRIT class for filters that can map to multiple user IDs.

The repeat count for the FLTRUSER field is stored in the FILTERCT field.

FSROOT

This field is found on the OVM segment of the user profile. It contains the user's OpenExtensions file system root directory.

GAUDIT

Flag field that indicates the global audit flags set by the auditor. This field is found in DATASET and general resource profiles. These flags determine whether to log successful and failed accesses.

The global audit qualifiers determine the level from which accesses are logged. These values are listed in the GAUDITQF and GAUDITQS fields. See also the AUDIT field, which lists the audit flags set by the user. The easiest way to print the global audit information is through the "GAUDITLVL" on page 1166 field, "GAUDITS" on page 1167, or "GAUDITF" fields.

Use the GAUDITLVL field if you want to permit authorized users to change audit field values on the display panels.

Table 399 lists the GAUDIT values and their meaning.

Table 399. GAUDIT values and descriptions

GAUDIT value	Meaning
ALL	Audit successful accesses from GAUDITQS and failed accesses from GAUDITQF.
SUCCESS	Audit successful accesses from GAUDITQS.
FAILURE	Audit failed accesses from GAUDITQF.
NONE	No auditing.

The audit qualifiers determine the level from which accesses are logged. These qualifiers are listed in the "GAUDITQF" on page 1166 and "GAUDITQS" on page 1166 fields (in non-interpreted form) and in the "GAUDITF" and "GAUDITS" on page 1167 fields (in common form).

The GAUDITQF and GAUDITQF fields are unpredictable when failure or success auditing has not been specified. For normal situations use GAUDITLVL, GAUDITS or GAUDITF. Use the GAUDITLVL field if you want to permit authorized users to change audit field values on the display panels.

GAUDITF

This derived field contains the global audit failure level. The value is based on the raw GAUDIT and GAUDITQF fields. The values it can have are listed in the Table 400. The blank (*X'FF'*) value means that global failure auditing is not active. This field is designed for use in SELECT statements.

Use the "GAUDITLVL" on page 1166 field if you want to permit authorized users to change audit field values on the display panels.

Table 400. GAUDITF values and descriptions

GAUDITF value	Internal value (hex)
ALTER	03
CONTROL	02

Table 400. GAUDITF values and descriptions (continued)

GAUDITF value	Internal value (hex)
UPDATE	01
READ	00
(blank)	FF

GAUDITLVL

This field can only be used for output. It contains the global audit level (both successes and failures) in a three-character format: a success level, a blank, and a failure level. The audit levels can have the blank values (not set). The following audit levels can be returned:

- **R** (Read)
- **U** (Update)
- **C** (Control)
- **A** (Alter)

The GAUDITLVL field is the only modifiable global audit field. Use this field if you want to permit authorized users to change audit field values on the display panels.

GAUDITQF

Flag field that indicates the global audit failure qualifier. This field is found in DATASET and general resource profiles and indicates the global audit failure qualifier. If the GAUDIT field is set to *ALL* or *FAILURE*, all failed accesses with intended access equal or higher than this field are logged.

The GAUDITQF field is unpredictable when failure auditing has not been specified. Use the "GAUDITF" on page 1165 field instead. Use the "GAUDITLVL" field if you want to permit authorized users to change audit field values on the display panels.

Table 401 lists the GAUDITQF values.

Table 401. GAUDITQF values

GAUDITQF value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
NONE	FF

GAUDITQS

Flag field that indicates the global audit success qualifier. This field is found in DATASET and general resource profiles.

If the GAUDIT field is set to *ALL* or *SUCCESS*, all successful accesses with intended access equal or higher than this field are logged.

The GAUDITQS field is unpredictable when success auditing has not been specified. Use "GAUDITS" on page 1167 instead.

Use the "GAUDITLVL" field if you want to permit authorized users to change audit field values on the display panels.

The following table lists the GAUDITQS values:

Table 402. GAUDITQS values

GAUDITQS value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
NONE	FF

GAUDITS

This derived field contains the global audit success level. The value is based on the raw GAUDIT and GAUDITQS fields. The values it can have are listed in Table 403. The blank (*X'FF'*) value means that global success auditing is not active. This field is designed for use in SELECT statements.

Use the "GAUDITLVL" on page 1166 field if you want to permit authorized users to change audit field values on the display panels.

Table 403. GAUDITS values

GAUDITS value	Internal value (hex)
ALTER	03
CONTROL	02
UPDATE	01
READ	00
(blank)	FF

GENERIC

This field indicates whether the profile is generic. It can be used to select generic DATASET and GENERAL profiles. It can be specified as an attribute, for example SELECT GENERIC. When used for output, it contains the string 'GENERIC' if the profile was generic, and is blank otherwise.

GID

This field is found in group profiles and is part of the OMVS segment. It indicates the numerical group id used for z/OS UNIX. If the overtype option is active, you can suffix the number with an S–*1001S* for example), so the SHARED command keyword is added. You can also specify AUTO, which results in addition of the AUTOGID command keyword. The SHARED and AUTOGID command keywords are available in z/OS 1.4. or with APAR OW52135.

GROUPADSP

This is an alias of GRPADSP field.

GROUPAUDIT

This is an alias of GRPAUD field.

GROUPAUDITOR

This is an alias of GRPAUD field.

GROUPDS

This is an alias of GROUPDSN field.

GROUPDSN, GROUPDS

This field can only be used for SELECT/EXCLUDE processing. It is an alias for the FLAG1 field found in DATASET BASE segments. It indicates whether the profile covers group data sets, for example, whether the high-level qualifier is a group id. It can be specified as an attribute, for example., SELECT GROUPDSN. Its opposite is USERDSN.

GROUPGRPACC

This is an alias of the GRPGRPACC field.

GROUPN

This field is found in the ROLE class and is part of the TME segment. It is the count of groups associated with the role. These groups are listed in GROUPS.

GROUPNM

This field is found in DATASET profiles. It indicates then-current connect group of the user who created the data set profile.

GROUPOPER

This is an alias of the GRPOPER field.

GROUPOPERATIONS

This is an alias of the GRPOPER field.

GROUPREVOKE

This is an alias of the GRPREVOKE field.

GROUPS

This field is found in the ROLE class as part of the TME segment. It is a repeat group field; the repeat count is stored in the GROUPN field. It contains the list of groups associated with the role.

GROUPSP

This is an alias of the GRPSPEC field.

GROUPSPEC

This is an alias of the GRPSPEC field.

GROUPSPECIAL

This is an alias of the GRPSPEC field.

GRPACC

This field is an alias for the FLAG5 field found in USER BASE segments. It indicates whether the user has the user-GRPACC attribute. It can be specified as an attribute, e.g., SELECT GRPACC. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPACC.

If the GRPACC attribute applies, any group DATASET profile created by the user is automatically accessible to all users connected to the group; this is achieved by granting the group UPDATE access on the access list. GRPACC applies if the user has either user-GRPACC or group-GRPACC in the connect group.

On standard userid overviews, this field is usually shown as the second position in a group column headed AG (ADSP and GRPACC).

GRPADSP, GROUPADSP

When used for output, this field is an alias for the CGFLAG1 field found in USER BASE segments. It is repeated for every connect group and indicates whether the user has the group-ADSP attribute in the connect group. The alias GROUPADSP can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT GRPADSP. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPADSP.

If the group-ADSP attribute is set for the user's current connect group, any group data set created by the user is protected by a discrete profile with the CGUACC of the current connect group as UACC. Most installations with list-of-groups checking active do not set the group-ADSP attribute, because, counterintuitively, the group-ADSP attribute used is always the one for the current connect group for the user, as opposed to the one for the connect to the group for which the data set is defined. The group-ADSP attribute is only used if system-ADSP is in effect (due to SETROPTS ADSP). This is indicated by the ADSP field of NEWLIST TYPE=SYSTEM.

GRPAUD, GROUPAUDITOR, GROUPAUDIT, GRPAUDITOR

When used for output, this field is an alias for the CGGRPAUD field found in USER BASE segments in the RDS. It is repeated for every connect group and indicates whether the user has the group-AUDITOR attribute in the connect group. The aliases GROUPAUDITOR, GROUPAUDIT and GRPAUDITOR can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT GRPAUD. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPAUD. See also the AUDITOR field.

GRPAUDITOR

This is an alias of the GRPAUD field.

GRPGRPAC

This is an alias of GRPGRPACC field.

GRPGRPACC, GROUPGRPACC, GRPGRPAC

This field is an alias for the CGFLAG5 field found in USER BASE segments. It is repeated for every connect group and indicates whether the user has the GRPACC attribute in the connect group entry. (See the CGGRPCT field for a list of all fields in the Connect Group repeat group.) The alias GROUPGRPACC can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT GRPGRPACC. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPGRPACC.

If the group-GRPACC attribute is set for the user's current connect group (or the user has the user-GRPACC attribute), any group DATASET profile created by the user is made accessible to all users connected to the group by granting the group UPDATE access on the access list. Note that most installations with list-of-groups checking active do not set the group-GRPACC attribute, because, counterintuitively, the group-GRPACC attribute used is always the one for the current connect group for the user, as opposed to the one for the connect to the group for which the data set is defined.

GRPOP

This is an alias of the GRPOPER field.

GRPOPER, GROUPOPERATIONS, GROUPOPER, GRPOPERATIONS, GRPOP

When used for output, this field is an alias for the CGFLAG3 field found in USER BASE segments. It is repeated for every connect group and indicates whether the user has the group-operations attribute in the connect group. The aliases GROUPOPERATIONS, GROUPOPER, GRPOPERATIONS and GRPOP can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT GRPOPER. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPOPER.

GRPOPERATIONS

This is an alias of the GRPOPER field.

GRPREVOK

This is an alias of the GRPREVOKE field.

GRPREVOKE, GROUPREVOKE, GRPREVOK

This field is found in USER BASE segments. It is repeated for every connect group and indicates whether the user has the REVOKE attribute in the connect group entry. It can be specified as an attribute, e.g., SELECT GRPREVOKE. This field takes the revoke date, resume date, and the date of the RACF database unload (or the current date for a database) into account as well as the revoked flag. Use the CGFLAG4 field to select on just the revoke flag. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPREVOKE.

GRPSPEC, GROUPSPECIAL, GROUPSPEC, GROUPSP, GRPSPECIAL, GRPSP

When used for output, this field is an alias for the CGFLAG2 field found in USER BASE segments. It is repeated for every connect group and indicates whether the user has the group-special attribute in the connect group. Its main names are GRPSPEC and GRPSPECIAL; the aliases GROUPSPECIAL, GROUPSPEC, GROUPSP and GRPSP can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT GRPSPEC. Its opposite for the purpose of SELECT/EXCLUDE processing is NOGRPSPEC.

HANDSHAKE

This flag field can only be found in the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY. It indicates whether the asymmetric key controlled by these profiles can be used to protect communication channels. You can use overriding format $NO for command generation in combination with the ASYMUSAGE keyword. See also “CSFAUSE” on page 1154.

HAS_PASSWORD

This flag field indicates that the user can use a password to logon.

HAS_PHRASE

This flag field indicates that the user can use a password phrase to logon.

On standard userid overviews, this field is usually shown as the second position in a group column headed EPEM (the first E means the user has a password envelope; P means the user has a password phrase; the next E means the user has a password phrase envelope; M means that password checks for the user are case-sensitive).

HAS_PPHENV

This flag field indicates that the user profile contains a password envelope with a form of the password that can be decrypted–that is, a two-way encrypted password.

HAS_PWDENV

This flag field indicates that the user profile contains a password envelope with a form of the password that can be decrypted–that is, a two-way encrypted password.

HEXKEY

The profile name (key) as it exists in the RACF database (for example, generic characters have not been converted). For SELECT/EXCLUDE processing, this can be used to search for specific internal values or specific generic characters.

For output, the default output format is in hexadecimal, with a default length of 88 characters, though a hexadecimal representation can be up to 512 characters long. Use the KEY field for the profile key in external format. The difference between HEXKEY and KEY(HEX,88) is that the former is in RACF internal format and the latter is a hexadecimal representation of the external (human-readable) format.

HOME

This field is found in user profiles and is part of the OMVS segment. It indicates the home directory used for z/OS UNIX. The home directory is a case-sensitive character string of up to 1024 characters.

HOMECELL

This field is found on the DCE segment of the user profile. It contains the home cell for this DCE user.

HOMEUUID

This field is found on the DCE segment of the user profile. It contains the home cell universal unique identifier. The UUID is exactly 36 characters, in the format *nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn* where n is any hexadecimal digit.

IC

This field is found in user profiles and is part of the NETVIEW segment. It contains the Initial Command to be executed by Netview whenever the operator logs on to Netview.

IDIDMAP_CMD_FILTER

Pseudo field found in IDIDMAP profiles that contains the identity filter. This field is intended to be used when generating RACMAP commands in CARLa. It is equivalent to KEY, except that quotes are doubled and `OPTION MY_CCSID=`*`ccsid`* has no influence on the output from this field: Conversion to EBCDIC always uses code page 1047. This field can only be used for output and for selection with EXISTS and MISSING (See “Selecting on field existence” on page 886.)

IDIDMAP_CMD_REGISTRY

Repeat group pseudo field that is equivalent to `DIDRNAME`, except that quotes are doubled and o`OPTION MY_CCSID=`*`ccsid`* has no influence on the output from this field. Conversion to EBCDIC always uses code page 1047. This field is intended to be used when generating RACMAP commands in CARLa. This field can only be used for output and for selection with `EXISTS` and `MISSING` keywords. (See “Selecting on field existence” on page 886.)

IDSTAR

Variable defined in C2RXDEF1 reflects the unconditional access given to `ID(*)`–all `userids` defined to RACF. See UACC for access given to all userids (even undefined ones).

INITCNT

This field is found in group profiles. It has no meaning.

INRANGE

This field is a flag that indicates whether the profile is in the proper RACF data set according to the RACF range table ICHRRNG (loaded from CKFREEZE or live when processing live RACF). This flag is always on unless you have specified SUPPRESS ICHRRNG to include profiles that are not in the proper data set.

INSTDATA, DATA

Installation data. Available in GROUP, USER, DATASET, and GENERAL profiles. Up to 255 characters.

The DATA field name can only be used for SELECT/EXCLUDE processing.

IS_GRPAUDIT, IS_GRPAUD

This pseudo field is only present for user profiles. It indicates whether the user has been connected to any group with the group-auditor attribute.

IS_GRPOPER

This pseudo field is only present for user profiles. It indicates whether the user has been connected to any group with the group-operations attribute.

IS_GRPSPEC, IS_GRPSPECIAL

This pseudo field is only present for user profiles. It indicates whether the user has been connected to any group with the group-special attribute.

JOBNAMES

For GENERAL profiles, this repeated field in the DLFDATA segment contains the `jobname` of the jobs that can access the `DLF` objects protected by the profile. The `jobname` might end in an asterisk (*) to indicate generic job names. The number of job names is listed in the JOBNMCNT field.

JOBNMCNT

For GENERAL profiles, this is a field in the DLFDATA segment containing the number of job names listed in the JOBNAMES field.

KERB

This field can only be used for SELECT/EXCLUDE processing. It selects KERB segments.

KERBNAME

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains either the Kerberos principal name for a user, or the unqualified Kerberos realm name for a general resource.

KERBREGISTRY, KERBREG

This field is found in the EIM segment of LDAPBIND and FACILITY class general resource profiles. On the IRR.PROXY.DEFAULTS profile in the FACILITY class it specifies the name of the Kerberos registry in the EIM domain that the system is configured to use. On other profiles it is ignored. This field supports the `overtype` option which permits authorized users to change the field value from an ISPF panel.

KEY, PROFILE

The profile name (key) in external format. That is, generic characters have been converted according to the EGN settings for the site. The length of this field can be up to 255 characters for general resource profiles; data set profiles are limited to 44 characters, and user and group profiles are limited to 8 characters. The default output length is 44 characters. Use the HEXKEY field for the internal format.

KEYDATE

For GENERAL profiles, this field in the SESSION segment lists the last date the session key was changed.

KEYFROM

This field is found in the KERB segment of the user profile. It indicates whether the password or the passphrase was used to generate the Kerberos key.

KEYINTVL

For GENERAL profiles, this field in the SESSION segment lists the number of days before the session key expires.

LANGUAGE

This field can only be used for SELECT/EXCLUDE processing. It selects LANGUAGE segments.

LAST_CONNECT_DATE

This derived field is only defined for user profiles. It contains the last RACINIT date for any group the user is connected to (it is the maximum of the repeated value CGLJDATE). This is usually a better estimate for the last logon date than the LJDATE (which is for instance also affected by ALTUSER), although deleting a user's most recent logon group can set this date back. Note that RACF uses the LJDATE to calculate the user's inactivity interval.

LCHGDAT

This date field is found in DATASET and GENERAL profiles and indicates the date the data set/resource was last updated.

LDAPHOST

This field is found on the PROXY segment of USER and FACILITY class general resource profiles. It specifies the URL of the LDAP server which the z/OS LDAP Server contacts when acting as a proxy on behalf of a requester.

LDAPPROF

This field is found on the EIM segment of the USER class. It specifies the name of a profile in the LDAPBIND class which contains the name of an EIM domain, to be used to establish a connection with the EIM domain.

LEVEL

This numeric field is present in DATASET and general resource profiles. Accepted integer values are 0 - 99. This field is not used by RACF; it is a field that an organization can use for any purpose.

LJDATE

This field, which is only found in user profiles, contains the user's last use date; usually this reflects the user's last logon date, but there is a class of profile updates that also affects this field. The accompanying time is found in the field LJTIME.

Another estimate of the last logon date is available in the field LAST_CONNECT_DATE, which is the maximum of the values in the CGLJDATE repeat group, and thus the date of the user's last RACINIT with any of his current connect groups. Note that this date might be set back to when the connect group last used for logon is deleted.

See also the CGLJDATE field.

LJTIME

This field is found in user profiles. It can only be used for output.It indicates the user's last logon time (the date of last logon is listed in LJDATE). See also the CGLJTIME field.

LNOTES

This field can only be used for SELECT/EXCLUDE processing. It selects LNOTES segments.

LOCALREGISTRY, LOCALREG

This field is found on the EIM segment of LDAPBIND and FACILITY class general resource profiles. On the IRR.PROXY.DEFAULTS profile in the FACILITY class it specifies the name of the local RACF registry in EIM domains. On IRR.ICTX.DEFAULTS[.*sysid*][profiles in the LDAPBIND class, this field specifies the registry used by the ICTX identity cache. On other profiles it is ignored. This field supports the `overtype` option which allows authorized users to change the field value from an ISPF panel.

LOGDAYS

For user profiles, this bit field lists the number of days a user cannot logon. For GENERAL profiles, this bit field listing the days a terminal cannot be used. See also the LOGTIME and LOGZONE fields. This field can only be used for output.

LOGTIME

For user profiles: a field listing the time of day a user can logon. For GENERAL profiles, you can use a field listing the time of day a terminal can be used. The output format of this field is *HHMM:HHMM* indicating the `starttime` and `endtime` when users have access, or *ANYTIME* if there are no time restrictions. See also the LOGDAYS and LOGZONE fields. This field can only be used for output.

LOGZONE

For GENERAL profiles, this field returns the time zone in which a terminal is located. The format of this field is 'E HH.MM' or 'W HH.MM'. This field can only be used for output.

LREFDAT

This date field is found in DATASET and GENERAL profiles and indicates the date the data set/resource was last referenced. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS).

MAGSTRIP

The operator identification associated with a user; only found in user profiles.

MAPPINGTIMEOUT,MAPTIMEO

This field is found in the ICTX segment of IRR.ICTX.DEFAULTS.** profiles in the LDAPBIND general resource class. It specifies the time (1-3600 seconds) the Identity Context Extension (ICTX) stores an identity mapping. This field supports `overtype` option.

MAPREQUIRED, MAPREQ

This field is found in the ICTX segment of IRR.ICTX.DEFAULTS.** profiles in the LDAPBIND general resource class. It specifies whether the Identity Context Extension (ICTX) requires identity mapping to a z/OS user ID. This field supports the `overtype` option which allows authorized users to change the field value from an ISPF panel.

MASK

This is an alias of FILTER field.

MATCH

This field can only be used for SELECT/EXCLUDE processing. It is used to search for all profiles that could match the resource name specified. The result includes both discrete and generic profiles; however, the indicated bit and the volume serials are ignored. This keyword is useful to determine what profiles would protect a resource if another profile was deleted. To search for an exact profile key, use the KEY field instead. To search using a generic pattern name, use the FILTER field instead.

For grouping profiles, the match is on the *member list* of the grouping profile. If a CLASS keyword is specified for a member class, the grouping class is automatically included. This allows selection of all profiles that could protect a CICS transaction; see also the examples at the end of this section.

Note that, if both the CLASS and MATCH keywords are specified, these two keywords should be the *first* keywords used in the SELECT/EXCLUDE statement or WHERE clause.

MAXTKTLF

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the maximum ticket life in seconds that is granted when generating a ticket for the target user or realm.

MAXFAIL

For GENERAL profiles: field in the SESSION segment listing the maximum number of invalid attempts before lockout.

MEMBERCLASS

For grouping profiles, this field contains the name of the corresponding member class. For a member profile, this field contains the name of the 'normal' profile class. For all other profile types, this field is undefined.

MEMBERKEY

This field can only be used for output. For grouping profiles, this repeated field contains the profile keys of all members. For all member profiles, this field contains the name of the 'normal' profile key. For all other profile types, this field is undefined.

MEMCNT

The number of members for a profile from a grouping class. The member class can be found using MEMBERCLASS. The MEMLST field lists the member profiles. Only found in GENERAL profiles.

MEMLIMIT

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum number of bytes of non-shared memory that can be allocated by the user. It is a numeric value between 0 and 16 777 215, followed by the letter M, G, T, or P. The M, G, T or P stand for megabyte, gigabyte, terabyte and petabyte, respectively. This field supports the `overtype` option which permits authorized users to change the value from an ISPF panel.

MEMLST

The member list of a general resource from a grouping class. This is a repeated field; each entry can be up to 255 characters. The member class can be found using MEMBERCLASS. The MEMCNT field lists the number of members. Only found in GENERAL profiles.

MGMTCLAS

For GROUP and user profiles: DFP-management class in DFP segment.

MINTKTLF

This field can be found in the KERB segment for the REALM General Resource class. It contains the minimum ticket life in seconds that is granted when generating a ticket for the target realm.

MMAPAREAMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum amount of data space storage (in pages) that can be allocated for memory mappings of HFS files. It lies between 1 and 16,777,216.

MODEL

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 1 in the DSTYPE field found in DATASET BASE segments. It indicates whether the profile is a model profile. It can be specified as an attribute, e.g., SELECT MODEL. Its opposite for the purpose of SELECT/EXCLUDE processing is NOMODEL. See also the DSTYPE field.

MODELNAM

The name of the data set model profile used to model new data set profiles created for the user or group. Up to 44 characters; only found in USER and group profiles.

MSGRECVR

This field is found in user profiles and is part of the NETVIEW segment. It contains a flag that indicates whether the operator can receive unsolicited Netview messages.

NAME

This is an alias of PGMRNAME (see “PGMRNAME” on page 1189).

NDS

This field can only be used for SELECT/EXCLUDE processing. It selects NDS segments.

NDSLINK_USERID

For a profile in the NDSLINK class, this field contains the userid this link is related to; for other classes it is always absent. When present, the content of this field is identical to that of the APPLDATA field.

NETVIEW

This field can only be used for SELECT/EXCLUDE processing. It selects NETVIEW segments.

NGMFADMN

This field is found in user profiles and is part of the NETVIEW segment. It contains a flag that indicates whether the operator can use the Netview Graphic Monitor Facility (NGMF).

NGMFVSPN

This field is found on the NETVIEW segment of the user profile. It contains the NetView Graphic Monitor Facility view span options.

NMAPCT

This field can be found in the BASE segment of the user profile. It is the count of digital certificate filters that map to this userid. The filter descriptions are listed in the NMAPNAME field, their labels in the NMAPLABL field.

NMAPLABL

This field is found in the BASE segment of the user profile. It is a repeat group field; its count is stored in the NMAPCT field. It shows the list of labels describing the digital certificate filters that map to this userid.

NMAPNAME

This field is found in the BASE segment of the user profile. It is a repeat group field; its count is stored in the NMAPCT field. It contains a list of the keys for the general resource profiles that describe the filters that map to this userid.

NO0LEVEL

Variable defined in C2RXDEF1 that is equivalent to `LEVEL`, except that it is missing when `LEVEL` is 0.

NOADSP

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the ADSP field. It selects user BASE segments for users that do no have the ADSP attribute. It can be specified as an attribute, e.g., SELECT NOADSP.

NOAUDITOR

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the AUDITOR field. It selects user BASE segments for users that do no have the system-auditor attribute. It can be specified as an attribute, e.g, SELECT NOAUDITOR.

NOAUTO

This is an alias of NOAUTOTAPE (see “NOAUTOTAPE”).

NOAUTOTAPE, NONAUTOTAPE, NOTAUTOTAPE, NOAUTO, NONAUTO, NOTAUTO

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the AUTOTAPE field. It selects TAPEVOL BASE segments for profiles that are not automatic TAPEVOL profiles. It can be specified as an attribute, e.g., SELECT NOAUTOTAPE. See also the RESFLG field.

NOCDTINFO

This field can only be used for SELECT/EXCLUDE processing. It selects non-CDTINFO segments.

NOCERTDATA

This field can only be used for SELECT/EXCLUDE processing. It selects non-CERTDATA segments.

NOCICS

This field can only be used for SELECT/EXCLUDE processing. It selects non-CICS segments.

NODCE

This field can only be used for SELECT/EXCLUDE processing. It selects non-DCE segments.

NODFP

This field can only be used for SELECT/EXCLUDE processing. It selects non-DFP segments.

NODLFDATA

This field can only be used for SELECT/EXCLUDE processing. It selects non-DLFDATA segments.

NOEIM

This field can only be used for SELECT/EXCLUDE processing. It selects non-EIM segments.

NOERASE

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the ERASE field. It selects DATASET BASE segments for profiles that do no have the erase-on-scratch flag set. That is, data sets that are not erased on scratch even if SETROPTS ERASE has been specified (without overriding suboperands). It can be specified as an attribute, e.g., SELECT NOERASE.

NOFAILLOAD

This field can only be used for SELECT/EXCLUDE processing. It selects non-FAILLOAD segments.

NOGROUPADSP

This is an alias of NOGRPADSP (see "NOGRPADSP" on page 1179).

NOGROUPAUDIT

This is an alias of NOGRPAUD (see "NOGRPAUD" on page 1179).

NOGROUPAUDITOR

This is an alias of NOGRPAUD (see "NOGRPAUD" on page 1179).

NOGROUPGRPACC

This is an alias of NOGRPGRPACC (see "NOGRPGRPACC" on page 1179).

NOGROUPOP

This is an alias of NOGRPOPER (see "NOGRPOPER" on page 1179).

NOGROUPOPER

This is an alias of NOGRPOPER (see "NOGRPOPER" on page 1179).

NOGROUPOPERATIONS

This is an alias of NOGRPOPER (see “NOGRPOPER”).

NOGROUPREVOKE

This is an alias of NOGRPREVOKE (see “NOGRPREVOKE” on page 1180).

NOGROUPSP

This is an alias of NOGRPSPEC (see “NOGRPSPEC” on page 1180).

NOGROUPSPEC

This is an alias of NOGRPSPEC (see “NOGRPSPEC” on page 1180).

NOGROUPSPECIAL

This is an alias of NOGRPSPEC (see “NOGRPSPEC” on page 1180).

NOGRPACC

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPACC field. It selects USER BASE segments for users that do no have the system-GRPACC attribute. It can be specified as an attribute, e.g., SELECT NOGRPACC.

NOGRPADSP, NOGROUPADSP

This repeated field can only be used for SELECT/EXCLUDE processing,and acts as an opposite to the GRPADSP field. It selects USER BASE segments for users that have at least one connect group without the group-ADSP attribute. (To select USER BASE segments without any group-ADSP attribute, use NOT(GRPADSP) instead.) It can be specified as an attribute, e.g., SELECT NOGROUPADSP.

NOGRPAUD, NOGROUPAUDITOR, NOGROUPAUDIT, NOGRPAUDITOR, NOGRPAUDIT

This repeated field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPAUD field. It selects USER BASE segments for users that have at least one connect group without the group-auditor attribute. (To select USER BASE segments without *any* group-auditor attribute, use NOT(GRPAUD) instead.) It can be specified as an attribute, e.g., SELECT NOGRPAUD.

NOGRPAUDIT

This is an alias of NOGRPAUD (see “NOGRPAUD”).

NOGRPAUDITPR

This is an alias of NOGRPAUD (see “NOGRPAUD”).

NOGRPGRPACC, NOGROUPGRPACC

This repeated field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPGRPACC field. It selects USER BASE segments for users that have at least one connect group without the group-GRPACC attribute. (To select USER BASE segments without *any* group-GRPACC attribute, use NOT(GRPGRPACC) instead.) It can be specified as an attribute, e.g., SELECT NOGRPGRPACC.

NOGRPOP

This is an alias of NOGRPOPER (see “NOGRPOPER”).

NOGRPOPER, NOGROUPOPERATIONS, NOGROUPOPER, NOGROUPOP, NOGRPOPERATIONS, NOGRPOP

This repeated field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPOPER field. It selects USER BASE segments for users that have at least one connect group without the group-operations attribute. (To select USER BASE segments without *any* group-operations attribute, use NOT(GRPOPER) instead.) It can be specified as an attribute, e.g., SELECT NOGRPOPER.

NOGRPOPERATIONS

This is an alias of NOGRPOPER (see "NOGRPOPER" on page 1179).

NOGRPREVOKE, NOGROUPREVOKE

This repeated field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPREVOKE field. It selects USER BASE segments for users that have at least one unrevoked connect group. This field takes the revoke date, resume date, and the date of the RACF database unload (or the current date for a database) into account as well as the revoked flag. Use the CGFLAG4 field to select on just the revoke flag. (To select USER BASE segments without any revoked connects, use NOT(GRPREVOKE) instead.) It can be specified as an attribute, e.g., SELECT NOGRPREVOKE.

NOGRPSP

This is an alias of NOGRPSPEC (see "NOGRPSPEC").

NOGRPSPEC, NOGROUPSPEC, NOGROUPSP, NOGRPSPECIAL, NOGROUPSPECIAL, NOGRPSP

This repeated field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the GRPSPEC field. It selects USER BASE segments for users that have at least one connect group without the group-special attribute. (To select USER BASE segments without *any* group-special attribute, use NOT(GRPSPEC) instead.) It can be specified as an attribute, e.g., SELECT NOGRPSPEC.

NOGRPSPECIAL

This is an alias of NOGRPSPEC (see "NOGRPSPEC").

NOKERB

This field can only be used for SELECT/EXCLUDE processing. It selects non-KERB segments.

NOLANGUAGE

This field can only be used for SELECT/EXCLUDE processing. It selects non-LANGUAGE segments.

NOLNOTES

This field can only be used for SELECT/EXCLUDE processing. It selects non-LNOTES segments.

NOMODEL

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the MODEL field. It selects DATASET BASE segments for profiles that are not model profiles. It can be specified as an attribute, e.g., SELECT NOMODEL. See also the DSTYPE field.

NONAUTO

This is an alias of NOAUTOTAPE (see "NOAUTOTAPE" on page 1177).

NONAUTOTAPE

This is an alias of NOAUTOTAPE (see “NOAUTOTAPE” on page 1177).

NONDS

This field can only be used for SELECT/EXCLUDE processing. It selects non-NDS segments.

NONETVIEW

This field can only be used for SELECT/EXCLUDE processing. It selects non-NETVIEW segments.

NONREVOKED

This is an alias of NOREVOKE (see “NOREVOKE” on page 1182).

NONVSAM

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the VSAM field. It selects DATASET BASE segments for profiles that are not VSAM data set profiles. It can be specified as an attribute, e.g., SELECT NONVSAM. See also the DSTYPE field.

NOOIDCARD, NOOID

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the OIDCARD field. It selects USER BASE segments for users that do not require an OID card to logon. It can be specified as an attribute, e.g., SELECT NOOIDCARD.

NOOMVS

This field can only be used for SELECT/EXCLUDE processing. It selects non-OMVS segments.

NOOPER

This is an alias of NOOPERATIONS (see “NOOPERATIONS”).

NOOPERATIONS, NOOPER

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the OPERATIONS field. It selects USER BASE segments for users that do no have the system-operations attribute (and CONNECT profiles that do not have the group-operations attribute). It can be specified as an attribute, e.g., SELECT NOOPERATIONS.

NOOPERPARM

This field can only be used for SELECT/EXCLUDE processing. It selects non-OPERPARM segments.

NOOVM

This field can only be used for SELECT/EXCLUDE processing. It selects non-OVM segments.

NOPASSWORD

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the PASSWORD field. It selects USER BASE segments for users that do not require a password to logon. It can be specified as an attribute, e.g, SELECT NOPASSWORD.

NOPROTECTED

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the PROTECTED field. It selects USER BASE segments for users that

are not protected, for example, that can be revoked for too many invalid password attempts. It can be specified as an attribute, for example, SELECT NOPROTECTED.

NOPROXY

This field can only be used for SELECT/EXCLUDE processing. It selects non-PROXY segments.

NORESTRICTED

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the RESTRICTED field. It selects USER BASE segments for users that are not restricted, for example, that can be granted access through the Global Access Table, the UACC of a profile, or ID(*). It can be specified only as an attribute, for example,SELECT NORESTRICTED.

NOREVOKE, NONREVOKED, NOTREVOKED

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the REVOKE field. It selects USER BASE segments for users that are not revoked. This field takes the revoke date, resume date, and the date of the RACF database unload (or the current date for a database) into account as well as the revoked flag. Use FLAG4 (or CGFLAG4) to select based on the revoke flag only. It can be specified as an attribute, e.g., SELECT NOREVOKE.

NOSESSION

This field can only be used for SELECT/EXCLUDE processing. It selects non-SESSION segments.

NOSIGAUDIT

This field can only be used for SELECT/EXCLUDE processing. It selects segments which do non-SIGREQUIRED segments.

NOSIGREQUIRED

This field can only be used for SELECT/EXCLUDE processing. It selects non-SIGREQUIRED segments.

NOSIGVER

This field can only be used for SELECT/EXCLUDE processing. It selects non-SIGVER segments.

NOSINGLEDS

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the SINGLEDS field. It selects TAPEVOL BASE segments for profiles that do not have the single-data set flag set. It can be specified as an attribute, e.g., SELECT NOSINGLEDS. See also the RESFLG field.

NOSPEC

This is an alias of NOSPECIAL (see “NOSPECIAL”).

NOSPECIAL, NOSPEC

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the SPECIAL field. It selects USER BASE segments for users that do no have the system-special attribute. It can be specified as an attribute, e.g., SELECT NOSPECIAL.

NOSTDATA

This field can only be used for SELECT/EXCLUDE processing. It selects non-STDATA segments.

NOSVFMR

This field can only be used for SELECT/EXCLUDE processing. It selects non-SVFMR segments.

NOTAPE

This is an alias of NOTAPEDSN (see “NOTAPEDSN”).

NOTAPEDSN, NOTAPE

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the TAPEDSN field. It selects DATASET BASE segments for profiles that are not tape data set profiles. It can be specified as an attribute, e.g., SELECT NOTAPEDSN. See also the DSTYPE field.

NOTAUTO

This is an alias of NOAUTOTAPE (see “NOAUTOTAPE” on page 1177).

NOTAUTOTAPE

This is an alias of NOAUTOTAPE (see “NOAUTOTAPE” on page 1177).

NOTELINK_USERID

NOTERM

This is an alias of NOTERMUACC (see “NOTERMUACC”).

NOTERMUACC, NOTERM

This field can only be used for SELECT/EXCLUDE processing. It is found in GROUP BASE segments. It indicates the NOTRMUAC attribute, i.e, terminal access is not granted through the UACC of terminal profiles, but only through access list entries. It can be specified as an attribute, e.g., SELECT NOTERMUACC. Its opposite is TERMUACC.

NOTIFY

This field is found in DATASET and GENERAL profiles and indicates the user to notify when access violations occur for a data set or resource protected by the profile.

NOTME

This field can only be used for SELECT/EXCLUDE processing. It selects non-TME segments.

NOTREVOKED

This is an alias of NOREVOKE (see “NOREVOKE” on page 1182).

NOTRMUAC

For group profiles: terminal UACC. See also the CGNOTUAC field and NOTERMUACC fields.

NOTSO

This field can only be used for SELECT or EXCLUDE processing. It selects non-TSO segments.

NOTVTOC

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the TVTOC field. It selects TAPEVOL BASE segments for profiles that do not have a TVTOC. It can be specified as an attribute, e.g., SELECT NOTVTOC. See also the RESFLG field.

NOUAUDIT

This field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the UAUDIT field. It selects USER BASE segments for users that are not being audited. It can be specified as an attribute, e.g, SELECT NOUAUDIT.

NOUNIVERSAL

This field can only be used for SELECT/EXPLODE processing and acts as an opposite to the UNIVERSAL field. It selects GROUP BASE segments for groups that are not universal, for example, that are limited to 5957 connected users. It can be specified as an attribute, for example, SELECT NOUNIVERSAL.

NOWARN

This is an alias of NOWARNING (see "NOWARNING").

NOWARNING, NOWARN

Indicates if the data set or resource has the NOWARNING attribute, which indicates that access is denied if other profile settings indicate that access is not permitted. If this attribute is set, it selects BASE segments for data set and general resource profiles that are not in WARNING mode. This field is found in the BASE segment of DATASET and general resource profiles. The value can be specified as an attribute, SELECT NOWARNING for example.

NOWORKATTR

This field can only be used for SELECT/EXCLUDE processing. It selects non-WORKATTR segments.

NUMCTGY

This field is found in USER, DATASET, and GENERAL profiles. It lists the number of security category entries. The security categories are listed in the CATEGORY field.

OID

This is an alias of OIDCARD (see "OIDCARD").

OIDCARD, OID

This field can only be used for SELECT/EXCLUDE processing. It corresponds to the FLAG8 field found in USER BASE segments. It indicates whether an OID card is required to logon. It can be specified as an attribute, e.g., SELECT OIDCARD. Its opposite is NOOIDCARD.

OLDPHR

Repeated field listing an encrypted previous password phrase. Only found in the BASE segment of user profiles. The previous password phrase generation number is listed in the OLDPHRNM field; the count of previous password phrase generations is listed in the PHRCNT field.

OLDPHRNM

Repeated field listing a previous password phrase generation number. Only found in the BASE segment of user profiles. The previous password phrase is listed in the OLDPHR field; the count of previous password phrase generations is listed in the PHRCNT field.

OLDPWD

Repeated field listing an encrypted previous password. Only found in the BASE segment of user profiles. The previous password generation number is listed in the OLDPWDNM field; the count of previous password generations is listed in the PWDCNT field.

OLDPWDNM

Repeated field listing a previous password generation number. Only found in the BASE segment of user profiles. The previous password is listed in the OLDPWD field; the count of previous password generations is listed in the PWDCNT field.

OMVS

This field can only be used for SELECT/EXCLUDE processing. It selects OMVS segments.

OPCLASS

This field is found in user profiles in the CICS and NETVIEW segments. It is a repeated field; the number of values is listed in the OPCLASSN field in the same segment.

In the CICS segment, it is a repeated field listing the user's operator classes. Each operator class value is a number in the range 1 to 24.

In the NETVIEW segment, it is a repeated field listing the Netview scope classes over which the operator has authority. Each scope class value is a number in the range 1 to 2040.

OPCLASSN

This field is found in user profiles in the CICS and NETVIEW segments. It indicates the number of CICS operator class values (CICS segment) or NETVIEW scope classes (NETVIEW segment), which are listed in the OPCLASS field in the same segment.

OPER, OPERATIONS

This field is an alias for the FLAG3 field found in USER BASE segments. It indicates whether the user has the system-operations attribute. It can be specified as an attribute, e.g., SELECT OPERATIONS. Its opposite for the purpose of SELECT/EXCLUDE processing is NOOPERATIONS.

On standard userid overviews, this field is usually shown as the second position in a group column headed SOA (SPECIAL, OPERATIONS, and AUDITOR).

OPERATIONS

This is an alias of OPER (see “OPER”).

OPERALTG

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the ALTGRP keyword, which indicates the alternative console group for recovery.

OPERAUTH

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the AUTH keyword, which indicates the operator's command authority.

OPERAUTO

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the AUTO flag, which indicates whether the console is to receive messages specified for automation through MPF.

OPERCMDS

This field is found in user profiles and is part of the OPERPARM segment. It contains the CMDSYS keyword, which indicates the name of the system that the operator is connected to for command processing.

OPERDOM

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the DOM keyword, which indicates whether the operator receives delete operator message requests.

OPERHC

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the HC keyword, which indicates whether the operator receives messages that are directed to hardcopy.

OPERINT

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the INTIDS keyword, which indicates whether the operator receives messages directed to console ID 0 (the internal console). Such messages are usually responses to internally issued commands.

OPERKEY

This field is found in user profiles and is part of the OPERPARM segment. It contains the KEY keyword, which indicates the retrieval key used for a DISPLAY CONSOLES command.

OPERLEVL

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the LEVEL keyword, which indicates the message level that the operator receives.

OPERLOGC

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the LOGCMDRESP flag, which indicates whether command responses are to be recorded on the hardcopy log.

OPERMCNT

This field is found in user profiles and is part of the OPERPARM segment. It lists the count of MSCOPE systems, which are listed in the OPERMSCP field.

OPERMFRM

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the MFORM keyword, which indicates the format in which messages are displayed.

OPERMGID

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the MIGID flag, which indicates whether the operator is to receive a migration console id.

OPERMON

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains the MONITOR keyword, which indicates the events that are monitored.

OPERMSCP

This field is found in user profiles and is part of the OPERPARM segment. It is a repeated field listing the MSCOPE systems, from which unsolicited messages are received. The number is listed in the OPERMCNT field.

OPERPARM

This field can only be used for SELECT/EXCLUDE processing. It selects OPERPARM segments.

OPERROUT

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the ROUTCODE keyword, which indicates the routing codes that are received.

OPERSTOR

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the STORAGE keyword, which indicates the maximum message queue storage in Mb.

OPERUD

This field is found in user profiles and is part of the OPERPARM segment. It can only be used for output. It contains a value for the UD keyword, which indicates whether *undeliverable* messages are received.

OPERUNKN

This field is found in user profiles and is part of the OPERPARM segment. It contains a value for the UNKNIDS keyword, which indicates whether the operator receives messages directed to unknown console IDs. Unknown consoles are typically one-byte console IDs that the system cannot unambiguously resolve.

OPIDENT

This field is found in user profiles and is part of the CICS segment. It indicates the user's operator identification code. The length of this field is 3.

OPPRTY

This field is found in user profiles and is part of the CICS segment. It indicates the user's operator priority value, which is a number in the range 0 to 255.

OPTIONS

This field is found on the EIM segment of LDAPBIND and FACILITY class general resource profiles. It specifies options that control the EIM configuration. This field supports the `overtype` option which permits authorized users to change the value from an ISPF panel.

OVM

This field can only be used for SELECT/EXCLUDE processing. It selects OVM segments.

OWNER, AUTHOR

The RACF user or group id of the profile's owner. Found in all profile types.

PACSCNT

Access count of a conditional access list entry. This number is only updated for discrete profiles, and only then if statistics are on (due to SETROPTS STATISTICS). This is a repeated field that can be combined with the PROGACS, USER2ACS, PROGRAM, and ACL2VAR fields. Found in DATASET profiles. The number of conditional access list entries is listed in the ACL2CNT field.

PADS

This field can only be used for SELECT/EXCLUDE processing and selects profiles in the PROGRAM class as well as data set profiles with a conditional access list. It can be specified as an attribute, for example, SELECT PADS.

PARENT

This field is found in the ROLE class as part of the TME segment. It is the parent role of this role.

PARMN

This field is found on the SVMR segment of the SYSMVIEW general resource profile. It contains the SystemView parameter name.

PASSASIS

This flag field is found in the BASE segment of user profiles and indicates that password checks for the user are case-sensitive.

On standard userid overviews, this field is usually shown as the last position in a group column headed EPEM (the first E means the user has a password envelope; P means the user has a password phrase; the next E means the user has a password phrase envelope; M means that password checks for the user are case-sensitive).

PASSDATE

A user's last password change date. Only found in the BASE segment of user profiles.

PASSINT

This field is only found inuser profiles and indicates the password interval in effect for the user. Valid interval values are 1 to 254; for any user, the lowest value of PASSINT and the system's password interval settings are used. The special value 255 (displayed as blank) indicates the user has a password that never expires.

PASSINT_EFFECTIVE

This field contains the effective password interval for a userid; it is in principle derived from the PASSINT field in the user profile and the SETROPTS PASSWORD(INTERVAL()) setting. Unless the user setting is NOINTERVAL (which is honored), RACF effectively uses the minimum of the two intervals. However, if this minimum is lower than the SETROPTS PASSWORD(MINCHANGE()) setting, the MINCHANGE setting is used instead. See also PASSWORD_EXPIRE_DATE and PASSWORD_EXPIRED.

Users that are assigned the PROTECT attribute cannot log on using a password; this field returns a missing value for these users.

PASSWORD

This field corresponds to the complement of the bit 0 in the FLAG7 field found in USER BASE segments. It indicates whether a password is required to logon. For SELECT/EXCLUDE processing, it can be specified as an attribute, e.g., SELECT PASSWORD. When used for output, it displays the encrypted password associated with the user. In an unloaded database, this field always contains asterisks. The user is not able to actually use the password to logon if he is also PROTECTED. The field's opposite for the purpose of SELECT/EXCLUDE processing is NOPASSWORD.

PASSWORD_EXPIRE_DATE

Contains the expiration date for the user password. Normally, this value is the sum of the last password change date and the effective password interval. PASSWORD_EXPIRE_DATE=NEVER selects users with NOINTERVAL. If you use an inequality operator in the selection criteria, include a separate EXCLUDE statement for the NEVER value.

User passwords that have explicitly been set to *expired* have an expiration date in the past. The last use date is returned if it is nonblank, as an estimate of when the password was set to *expired*. For a userid that has never been used, the creation date is returned in the PASSWORD_EXPIRE_DATE field. These values are returned so that these entries can be identified in queries to locate recently expired userids. See also PASSINT_EFFECTIVE and PASSWORD_EXPIRED.

Users assigned the PROTECT attribute cannot log on using a password; this field returns NEVER for these users.

PASSWORD_EXPIRED

This flag field indicates whether a userid has an expired password. This flag pertains to the unload date rather than today. To search for the password status as of today using an unload data set, specify the following query: PASSWORD_EXPIRE_DATE <>NEVER AND PASSWORD_EXPIRE_DATE<=TODAY. See also PASSWORD_EXPIRE_DATE and PASSINT_EFFECTIVE.

On standard userid overviews, this field is usually shown as the last position in a group column headed LCX which shows flag fields to indicate the following conditions.

L means the user has at least one RACLINK

C means the user has a certificate.

X means that the password for the user has expired.

PGMRNAME, NAME

User name (20 characters). This field is only available for profiles of class USER.

PHRASE

This field can only be found in the BASE segment of user profiles. It displays the encrypted password phrase associated with the user. In an unloaded database, this field always contains asterisks.

PHRASE_EXPIRED

This flag field indicates whether a userid has an expired password phrase. This flag pertains to the unload date rather than today; if you want to know about today's status, you can use a query like PHRASE_EXPIRE_DATE <>NEVER AND PHRASE_EXPIRE_DATE<=TODAY. See also PHRASE_EXPIRE_DATE, PASSINT_EFFECTIVE, PASSWORD_EXPIRE_DATE, and PASSWORD_EXPIRED.

PHRASE_EXPIRE_DATE

Contains the password phrase expiration date for the user. Normally, this value is the sum of the last password phrase change date and the effective password interval. PHRASE_EXPIRE_DATE=NEVER selects users that have no password interval specified (NOINTERVAL). If you use an inequality operator in the selection criteria, include a separate EXCLUDE statement for the NEVER value.

User password phrases that have explicitly been set to *expired* have an expiration date in the past. For these password phrases, the *last use date* is returned if it is nonblank to provide an estimate when the password phrase was set to expired. For userids that have never been used, the creation date is returned in the PHRASE_EXPIRE_DATE field. These values are returned so that these entries can be identified in queries to locate recently expired userids. See also PASSINT_EFFECTIVE, PHRASE_EXPIRED, PASSWORD_EXPIRE_DATE, and PASSWORD_EXPIRED.

Users assigned the PROTECT attribute cannot log on using a phrase; this field returns NEVER for these users.

PHRCNT

This field contains the count of previous password phrase generations. Only found in the BASE segment of user profiles. The previous password phrase generations are listed in the OLDPHRNM and OLDPHR fields. This field is only used if the SETROPTS PASSWORD(HISTORY) option is or was active.

PHRDATE

user profile

This field is found in the BASE segment of user profiles and it contains the user's last password phrase change date. Only found in the BASE of user profiles.

PHRGEN

Current password phrase generation number, from the BASE segment of a user profile.

PPHENV

This field lists the content of the Password Phrase Envelope field of a user profile. It contains a decrypted form of the user password phrase.That is, a two-way encrypted form of the phrase in contrast to the PHRASE field, which uses a one-way encrypted value.

By default this field is shown 40 characters long, as a text string with values that cannot be printed replaced with a period. This field can only be shown from a RACF database, it is masked in data from an UNLOAD file.

PREVKEY

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the previous key for the user or realm in encrypted form. This field is removed from any UNLOAD made.

PREVKEYV

This field can be found in the KERB segment for both the USER and the REALM General Resource class. It contains the version number of the previous key for the user or realm.

PROCUSERMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum number of processes that this user is permitted to have active at

the same time, regardless of how the process became a z/OS UNIX System Services process. It lies between 3 and 32,767.

PROFILE

This is an alias of KEY (see "key" on page 1172).

PROFILE_USED

This field is a flag that indicates whether RACF uses the profile in authorization checking or not. If the flag is No, you can use the field AUDITCONCERN in zSecure Audit for RACF to display the reason why the profile is not used. The reason can for instance stem from the router table, the class descriptor table, SETROPTS class settings, or the range table (if SUPPRESS ICHRRNG was specified).

PROFLEN

This field is defined for all profiles and contains the logical length of the profile (segment) in the RACF database, in bytes. Up to 7 digits.

PROFTYPE

This field can only be used for output. For general resource profiles, this results in a blank field (for discretes) or the word GENERIC (for generics). For data set profiles, this results in one of the words GENERIC, NONVSAM, VSAM, TAPEDSN, or MODEL. For USER, GROUP, and CONNECT profiles, the field is '**n/a**'.

PROGACS

The access level of a conditional access list entry. This is a repeated field that can be combined with the PACSCNT, USER2ACS, PROGRAM, and ACL2VAR fields. Found in DATASET profiles. The number of conditional access list entries is listed in the ACL2CNT field. The easiest way to display normal and conditional access list entries is the ACL combination field. The PROGACS field can have the following values:

- ALTER
- CONTROL
- UPDATE
- READ
- EXECUTE
- NONE

PROGRAM

The PROGRAM field is found in the BASE segment of DATASET profiles and in the OMVS segment of user profiles; it has a different meaning in the two profile types.

In DATASET profiles, it indicates the program name of a conditional access list entry. This is a repeated field that can be combined with the PROGACS, USER2ACS, PACSCNT, and ACL2VAR fields. The number of conditional access list entries is listed in the ACL2CNT field. The easiest way to display normal and conditional access list entries is the ACL combination field.

In user profiles, it indicates the start-up program or shell used for z/OS UNIX. The start-up program is a case-sensitive character string of up to 1024 characters.

PROTECTED

This field is found in USER BASE segments. It indicates if the user is protected. A protected user does not have a password or an `oidcard` and can only be used to enter the system in a way that does not support passwords. For example, the ID can be used for a started task. The specified user ID cannot be revoked for invalid password attempts. The `PROTECTED` value can be specified as an attribute, SELECT PROTECTED for example. Its opposite for the purpose of SELECT/EXCLUDE processing is NOPROTECTED.

On standard `userid` overviews, this field is usually shown as the last position in a group column headed RIRP (REVOKED, REVOKE_INACTIVE, RESTRICTED, and PROTECTED).

Note: RACF databases on z/OS have slightly different bit settings from those on z/VM. This field is meant for use on z/OS. See `PROTECTED_ZVM`.

PROTECTED_ZVM

Variable defined in C2RXDEF1 that is the equivalent of PROTECTED for RACF for z/VM databases.

PROXY

This field can only be used for SELECT/EXCLUDE processing. It selects PROXY segments.

PWDCNT

Field listing the count of previous password generations. Only found in the BASE segment of user profiles. The previous password generations are listed in the OLDPWDNM and OLDPWD fields. This field is only used if the SETROPTS PASSWORD(HISTORY) option is or was active.

PWDENV

This field lists the content of the Password Envelope field of a user profile. It contains a decrypted form of the user password. That is, the password is two-way encrypted. This field value is in contrast to the PASSWORD field, which is provides the password in a one-way encrypted form.

PWDGEN

Current password generation number, from the BASE segment of a user profile.

PWHASHED

This field can only be used on a RACF database, and is blank for an unloaded database. It is YES if the password has been encrypted using the hashing algorithm, NO otherwise. Note: There is a very remote possibility that this field is set to YES for a DES-encrypted password. In that case, two different passwords exist that both lead to the same encrypted passwords, one with the DES algorithm and one with the hashing algorithm. If your installation has the password encryption exit ICHDEX01 or ICHDEX11 set to migration, both passwords can be used to logon.

QUAL

The QUAL field on a LIST family command contains the first qualifier for data set and general resource profiles, and contains the profile key for user and group profiles. For data set profiles, *id* matches the first qualifier (as changed by ICHCNX00 and ICHNCV00).

On a SELECT family command it matches any profile if the class is not DATASET, and restricts class DATASET profiles to those with a matching first

qualifier as modified by ICHCNX00 and ICHNCV00. A field-field comparison, however, is **not** restricted to the DATASET class.

QUAL1

The QUAL1 field contains the first qualifier for data set and general resource profiles, and contains the profile key for user and group profiles. For data set profiles, *id* matches the actual first qualifier (*not* as changed by ICHCNX00).

RACLDSP

This field is defined in the BASE segment of the RACGLIST general resource class. It is used for RACLIST processing.

RACLHDR

This field is defined in the BASE segment of the RACGLIST general resource class. It is used for RACLIST processing.

RACLINK

This repeated field lists information in the user profile set by RACLINK. It lists the following columns: `linked node`, `remote userid`, type of the link record (*Peer*, *Slave*, or *Master*, status ('*Err*, *Pend*, or blank), whether passwords are to be synchronized (*Sync* or blank), time stamps for creation and approval (both in GMT in the format `yyyy/mm/dd hh:mm`, and creating `userid`. The linked node, link record type, and password fields are modifiable. Authorized users can edit the values for these fields interactively from the `RACLINK` section on the User Profile detail display panel. See "User profile detail display" on page 92.

See also the TUDATA field.

RACMAP_CMD_FILTER

Repeat group pseudo field that is equivalent to `DMAPNAME`, except that quotes are doubled and `OPTION MY_CCSID=`*`ccsid`* has no influence on the output from this field: Conversion to EBCDIC always uses code page 1047. This field is intended to be used when generating RACMAP commands in CARLa. This field can only be used for output and selection with the EXISTS and MISSING keywords. (See "Selecting on field existence" on page 886.)

RACMAP_CMD_REGISTRY

Repeat group pseudo field that is equivalent to `RACMAP_REGISTRY`, except that quotes are doubled and `OPTION MY_CCSID=`*`ccsid`* has no influence on the output from this field. Conversion to EBCDIC always uses code page 1047. This field is intended to be used when generating RACMAP commands in CARLa. This field can only be used for output and for selection with the EXISTS and MISSING keywords. (See "Selecting on field existence" on page 886.)

RACMAP_REGISTRY

This repeat group pseudo field is found in the `BASE` segment of user profiles. It contains the registries for the identity mappings to this userid. The repeat count is contained in the `DMAPCT` field. This field can only be used for output and for selection with `EXISTS` and `MISSING`. For additional information, see the following field descriptions: `DMAPCT`, `DIDRNAME`, `DMAPLABL`, and `RACMAP_CMD_REGISTRY`.

RBA

This field is defined for all profile types and contains the Relative Byte Address of the selected profile (segment) within the containing data set of the originating database. Together with the DB field, this uniquely identifies a profile

(segment). Its main use is to keep operating in situations where BAM conflicts are reported by IRRUT200, for instance by excluding profiles that are in use, but not present in the index.

RCVT_RACFLEVEL

This field indicates the software level of RACF in a four-character format, for example: '7705'. The RACFLEVEL format can be used to format the software level of RACF as an SMP /E FMID, for example: '7.7.5'.

This field can be used in a DEFINE statement to generate certain keywords if the RACF level satisfies a condition, for example:

```
DEFINE generate_shared(str$blank(' shared') 0) TRUE,WHERE RCVT_RACFLEVEL>='7705'
```

RECNO

This pseudofield is defined for all profiles in an UNLOAD. It contains the record number of the profile. For all profiles in a DATABASE, this pseudo field contains zero.

RECREATE_KEY

This field is used by an internal CARLa script (CKRXRDS) to reformat nine-character data set profile names terminated by an asterisk (*) into valid RACF profile names. Generic data set profile names such as AAA.ABCDEFGH*.** are rejected by the ADDSD command. A generic profile such as AAA.ABCDEFGH*, created without the EGN option, is converted to AAA.ABCDEFGH*.** when the enhanced generic name (EGN) option is activated. The CARLa script (CKRXRDS) uses the RECREATE_KEY field to strip out the extra asterisk (*) and create a valid name, for example AAA.ABCDEFGH.**

RESFLG

This flag field is found in TAPEVOL BASE segments. It can only be used for output processing. The output is a three-character field in the form SAT. The first character describes the SINGLEDSN flag, and is blank if this flag is not set, and 'S' if this flag is set. The second character describes the AUTOTAPE flag, and is blank if this flag is not set, and 'A' if this flag is set. The last character describes the TVTOC flag, and is blank if this flag is not set, and 'T' if this flag is set. For SELECT/EXCLUDE processing, use the SINGLEDS, AUTOTAPE, and TVTOC fields.

RESN

This field is found in the ROLE class and is part of the TME segment. It is the count of resource access specifications of the role. These resource access specifications are listed in RESOURCE.

RESOURCE

This field is found in the ROLE class as part of the TME segment. It is a repeat group field; the repeat count is stored in the RESN field. It contains the list of resource access specifications of the role.

RESOWNER

This field is only found in the DFP segment of DATASET profiles. It indicates the DFP-RESOURCE owner, for example, the group or user from which the DFP segment is used for the creation of a new data set.

RESTRICTED

This field is an alias for the FLAG9 field found in USER BASE segments. It indicates whether the user has the RESTRICTED attribute, for example, that the user cannot be granted access through the global access table, the UACC of a profile, or ID(*). It can be specified as an attribute, e.g., SELECT RESTRICTED. Its opposite for the purpose of SELECT/EXCLUDE processing is NORESTRICTED.

On standard userid overviews, this field is usually shown as the third position in a group column headed RIRP (REVOKED, REVOKE_INACTIVE, RESTRICTED, and PROTECTED).

RESUMEDT

Resume date of a user from the user profile or group-connect. Found in user profiles. See also the CGRESMDT field.

RETAIN

For GENERAL profiles, flag byte field in the DLFDATA segment that contains the retain setting which indicates whether the DLF object can be retained after use.

RETPD

This field is found in GENERAL profiles and can only be used for output. The retention period, for example, the number of days protection is provided for the tape data set. A numerical value in the range 0 to 65533, with the value 99999 indicating no expiration.

REVOKE, REVOKED

This field is found in USER BASE segments. It indicates whether the user is revoked. The alias REVOKED can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, e.g., SELECT REVOKE. This field takes the revoke date, resume date, and the date of the RACF database unload (or the current date for a database) into account as well as the revoked flag. Use the FLAG4 (or CGFLAG4) field to display just the revoke flag. The field's opposite for the purpose of SELECT/EXCLUDE processing is NOREVOKE.

On standard userid overviews, this field is usually shown as the first position in a group column headed RIRP (REVOKED, REVOKE_INACTIVE, RESTRICTED, and PROTECTED).

REVOKED

This is an alias of REVOKE (see “REVOKE”).

REVOKE_INACTIVE

This pseudo-field flag indicates whether the user would be revoked due to inactivity the moment he tried to logon or start a job. It takes into account the global SETROPTS INACTIVE setting and the user's last use date.

On standard userid overviews, this field is usually shown as the second position in a group column headed RIRP (REVOKED, REVOKE_INACTIVE, RESTRICTED, and PROTECTED).

REVOKECT

Count of unsuccessful password attempts. This field is only found in user profiles.

Note: RACF only updates this value if user-revokes are in effect because of a SETROPTS PASSWORD(REVOKE) command.

REVOKEDT

Revoke-by date of a user. Found in USER and CONNECT profiles. See also the CGREVKDT field.

RINGCT

This field can be found in the CERTDATA segment of the DIGTCERT general resource class. It is a count of the keyrings to which the digital certificate is connected.

RINGNAME

This field can be found in the CERTDATA segment of the DIGTCERT general resource class. It is a repeat group field; the repeat count is stored in the RINGCT field. It contains a list of full names (`userid` and `keyringname`) of the keyrings to which this digital certificate is connected.

RINGSEQN

This field can be found in the CERTDATA segment of the DIGTRING general resource class. It contains an automatically generated sequence number, defining the ring.

ROLEN

This field is found in GENERAL, GROUP and DATASET profiles and is part of the TME segment. It is the count of roles associated with the profile. These roles are listed in ROLES.

ROLES

This field is found in GENERAL, GROUP and DATASET profiles as part of the TME segment. It is a repeat group field; the repeat count is stored in the ROLEN field. It contains the list of roles associated with the profile.

RSLKEY

This repeated field is found in user profiles and is part of the CICS segment. It contains the Resource Security Level Keys that are assigned to the user. The number of RSLKEYs is stored in the RSLKEYN field. For administration purposes it is recommended to use the CICS_RSLKEY pseudo field instead, which supports command generation and the `overtype` option for changing field values from an ISPF panel.

RSLKEYN

This field is found in user profiles and is part of the CICS segment. It contains the number of Resource Security Level Keys that is assigned to the user. The keys themselves are listed in the RSLKEY field.

SALT

This field can be found in the KERB segment for the REALM General Resource class. It contains the seed used by this realm in its random generation processing. This field is removed from any UNLOAD made.

SCRIPTN

This field is found on the SVMR segment of the SYSMVIEW general resource profile. It contains the SystemView script name.

SEARCHKEY

This field contains the profile key in RACF sort order, for example, generic characters sort after alphanumerical characters. The main use of this field is to

change the sort order. Because it contains unprintable data, the NONDISPLAY output modifier is recommended. Sort RACF profiles in search order by making SEARCHKEY(NONDISPLAY) the first field of a SORTLIST/DISPLAY.

SECLABEL

User/data set/resource security label. This field is found in USER, DATASET, GENERAL profiles.

SECLEVEL

User/data set/resource security level. This field is found in USER, DATASET, and GENERAL profiles. For SELECT/EXCLUDE processing, a hexadecimal (internal) value must be specified.

SECUREEXPORT

Flag field that can only be found in the ICSF segment which specifies attributes for the keys controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY,and GXCSFKEY. It indicates whether the asymmetric key controlled by these profiles can be used to export or import symmetric keys. You can use overriding format $NO for command generation in combination with the ASYMUSAGE keyword. See also “CSFAUSE” on page 1154.

SEGCNT

This field is only found in very old (pre-RACF 1.9.2), so-called *non*-RDS, RACF databases, for all profile types. It indicates the number of segments included in the profile. The basic profile contents (which is called the BASE profile) is not counted as a segment. The segment names are listed in the SEGNAME field.

SEGMENT

This indicates the 8 character segment type of the selected profile segment, including BASE. Use the SEGNAME field to display all segment names from the profile.

For SELECT/EXCLUDE processing, this parameter selects the indicated segment types.

SEGNAME

This repeated field is only found in very old (pre-RACF 1.9.2), so-called *non*-RDS, RACF databases, for all profile types. It lists the names of the segments included in the profile. The basic profile contents (which is called the BASE profile) are not counted as a segment. The number of segment names that are listed is in the SEGCNT field.

SENTCNT

For GENERAL profiles: field in the SESSION segment containing the number of session entities. The entities are listed in the SENTITY and SENTFLCT fields.

SENTFLCT

For GENERAL profiles: field in the SESSION segment containing the number of failed attempts for the session entity. This is a repeated field that can be combined with the SENTITY field. The number of entities listed is in the SENTCNT field.

SENTITY

For GENERAL profiles: field in the SESSION segment containing the session entity name. This is a repeated field that can be combined with the SENTFLCT field. The number of entities listed is in the SENTCNT field.

SESSION

This field can only be used for SELECT/EXCLUDE processing. It selects SESSION segments.

SESSKEY

For GENERAL profiles: field in the SESSION segment containing the session key. This is an 8 byte DES key stored in clear text. The low-order bits of each byte are parity bits that do not change the actual key.

SHMEMMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum number of bytes of shared memory that can be allocated by the user. It is a numeric value between 0 and 16 777 215, followed by the letter M, G, T, or P. The M, G, T or P stand for megabyte, gigabyte, terabyte and petabyte, respectively. This field supports the `overtype` option.

SIGAUDIT

SIGAUDIT is found in GENERAL resource profiles and is part of the SIGVER segment. The value in this field indicates under what conditions RACF records an SMF type 80 record with qualifier code 86. The possible conditions are: `ALL`, `SUCCESS`, `ANYBAD`, `BADSIGONLY`, `NEVER`.

Table 404. Signature Verification validation - Conditions for logging

Value	Description
ALL	Specifies logging all signature verifications, whether successful or not.
SUCCESS	Specifies logging only signature verification successes.
ANYBAD	Specifies logging only signature verification failures, regardless of the cause.
BADSIGONLY	Specifies logging only signature verification failures caused by an incorrect digital signature.
NONE	Specifies that signature verification events are *never* to be logged.

SIGREQUIRED, SIGREQD

SIGREQUIRED is found in `GENERAL` resource profiles and is part of the `SIGVER` segment. This is a flag field that indicates whether a signature is required in order for a program to be loaded. This field can have the following values:

- `YES` specifies that a program protected by the profile must be digitally signed.
- `NO` specifies that a program protected by the profile need not be digitally signed.

Selection can be based on the value of the field or the presence of the field.

SIGVER

This is the name of an optional PROGRAM class GENERAL resource profile segment. This field can only be used for SELECT/EXCLUDE processing. It selects SIGVER segments.

SINGLEDS

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 0 in the RESFLG field found in TAPEVOL BASE segments. It indicates whether the single-data set flag is set. It can be specified as an attribute, e.g.,

SELECT SINGLEDS. Its opposite for the purpose of SELECT/EXCLUDE processing is NOSINGLEDS. See also the RESFLG field.

SLSFAIL

For general resource profiles, this field provides the current number of invalid attempts field. This field is in in the SESSION segment listing.

SLSFLAGS

For GENERAL profiles: flags in the SESSION segment. Currently, only one flag bit (bit 0) has been defined. If set, the profile is locked out.

SNAME

This field is found in user profiles and is part of the LNOTES segment. It indicates the Lotus Notes short name for this user. Care must be taken to ensure that this field has a unique value for each user.

SPEC

This is an alias of SPECIAL (see "SPECIAL").

SPECIAL, SPEC

This field is an alias for the FLAG2 field found in USER BASE segments. It indicates whether the user has the system-special attribute. It can be specified as an attribute, e.g., SELECT SPECIAL. Its opposite for the purpose of SELECT/EXCLUDE processing is NOSPECIAL.

On standard userid overviews, this field is usually shown as the first position in a group column headed SOA (SPECIAL, OPERATIONS, and AUDITOR).

SSKEY

This field is found in PTKTDATA profiles and is part of the SSIGNON segment. It contains an encrypted (or masked) 8 byte secure-signon key. The default display format is hex. An `UNLOAD` operation replaces this field by asterisks (X'5C').

STAMP

If the RACF database is an `UNLOAD` file, this field displays the local date and time of the `UNLOAD` operation. If the database is live, it displays current date and time. For a copy of a database, it is displayed as '00:00:00.000000'.

STDATA

This field can only be used for SELECT/EXCLUDE processing. It selects STDATA segments.

STGROUP

This field is found in STARTED profiles and is part of the STDATA segment. It contains the group id to be used for a started procedure matching the STARTED profile. The special value =MEMBER indicates that the started procedure name must be used as the groupid.

STORCLAS

For GROUP, user profiles: DFP-storage class in DFP segment.

STUSER

This field is found in STARTED profiles and is part of the STDATA segment. It contains the userid to be used for a started procedure matching the STARTED profile. The special value =MEMBER indicates that the started procedure name must be used as the userid.

SUBGRPCT

This field lists the number of subgroups. This field is only found in group profiles. The SUBGRPNM field lists the subgroups.

SUBGRPNM

This is a repeated field listing the subgroups of a group. This field is only found in group profiles. The SUBGRPCT field contains the number of subgroups.

SUPGROUP

The superior group of a group. This field is only found in group profiles.

SVFMR

This field can only be used for SELECT/EXCLUDE processing. It selects SVFMR segments.

SYMEXPORTABLE

See “CSFAUSE” on page 1154.

SYMEXPORTCERTS

See “CSFSCLBS” on page 1156.

SYMEXPORTKEYS

See the “CSFSKLBS” on page 1156.

SYMCPACFWRAP

See the CSFSCPW field.

TACCNT

This field is found in user profiles and is part of the TSO segment. It indicates the user's default account number.

TAPE

This is an alias of TAPEDSN. See “TAPEDSN.”

TAPEDSN, TAPE

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 2 in the DSTYPE field found in DATASET BASE segments. It indicates whether the profile is a tape data set profile. It can be specified as an attribute, e.g., SELECT TAPEDSN. Its opposite for the purpose of SELECT/EXCLUDE processing is NOTAPEDSN. For output, use the DSTYPE field.

TCOMMAND

This field is found in user profiles and is part of the TSO segment. It indicates the user's default command at logon.

It can be set using the CKGRACF FIELD command, or by the RACF ALTUSER command.

TCONS

This field is found in user profiles and is part of the TSO segment. It indicates the consoles support.

TDEST

This field is found in user profiles and is part of the TSO segment. It indicates the user's default output destination identifier.

TERMUACC

This flag field can only be used for SELECT/EXCLUDE processing and acts as an opposite to the NOTERMUACC field. It selects GROUP BASE segments without the NOTRMUAC attribute, for example, terminal access might be granted through the UACC of TERMINAL profiles. It can be specified as an attribute, for example, SELECT TERMUACC.

THCLASS

This field is found in user profiles and is part of the TSO segment. It indicates the user's default hold class.

THREADSMAX

This field is found in user profiles and is part of the OMVS segment. It indicates the maximum number of pthread_created threads, including those running, queued, and exited but not detached, that this user can have currently active. It lies between 0 and 100,000.

TIMEOUT

This field is found in user profiles and is part of the CICS segment. It indicates the user's terminal time-out value, which is the number of minutes a user must be inactive before CICS times out the terminal. This is a hh:mm value with mm in the range 0 to 59. Note that CICS rounds values up to the nearest multiple of 5. The length of this field is 5.

TJCLASS

This field is found in user profiles and is part of the TSO segment. It indicates the user's default job class.

TLPROC

This field is found in user profiles and is part of the TSO segment. It indicates the user's logon procedure.

TLSIZE

This field is found in user profiles and is part of the TSO segment. It indicates the user's logon region size, in units of 1024 bytes.

TMCLASS

This field is found in user profiles and is part of the TSO segment. It indicates the user's default message class for submitted jobs.

TME

This field can only be used for SELECT/EXCLUDE processing. It selects TME segments.

TMSIZE

This field is found in user profiles and is part of the TSO segment. It indicates the user's maximum region size, in units of 1024 bytes.

TOPTION

This field is found in user profiles and is part of the TSO segment. This field can only be used for output and displays TSO logon options in a 4 character field. It can be a combination of the letters MNRO for MAIL, NOTICE, RECOVER and OIDCARD, respectively.

TPERFORM

This field is found on the TSO segment of the user profile. It contains the performance group to which this user belongs.

TRBA

This field is found in user profiles and is part of the TSO segment. It indicates the RBA of the user's broadcast area (the offset within the SYS1.BRODCAST data set).

TREELINE

Internal sort key for a group-tree display. This field, which is only defined for group profiles, and might only be used with the SORTLIST, DISPLAY and (D)SUMMARY commands, indicates the position of the group within the group tree. This field does not result in 'pretty' output. Sort the group entries in a tree by making TREELINE(NONDISPL) the first field of a SORTLIST/DISPLAY.

TSCLASS

This field is found in user profiles and is part of the TSO segment. It indicates the user's default `sysout` class for printed output.

TSLKEY

This repeated field is found in user profiles and is part of the CICS segment. It contains the Transaction Security Level Keys that are assigned to the user. The number of TSLKEYs is stored in the TSLKEYN field. For administration purposes it is recommended to use the CICS_TSLKEY pseudofield instead, which supports command generation and the `overtype` option which permits authorized users to change the field value from an ISPF panel.

TSLKEYN

This field is found in user profiles and is part of the CICS segment. It contains the number of Transaction Security Level Keys that is assigned to the user. The keys themselves are listed in the TSLKEY field.

TSO

This field can only be used for SELECT/EXCLUDE processing. It selects TSO segments.

TSOSLABL

This field is found in user profiles and is part of the TSO segment. It indicates the default logon `seclabel` for the user.

TUCNT

This field is found in user profiles. It indicates the number of target userid entries. The entries are listed in the TUKEY and TUDATA fields.

TUDATA

This field is found in user profiles in the BASE and TSO segments.

In the TSO segment, it contains the TSO user data (carried over from SYS1.UADS). This field consists of 4 characters in the range 0-9 and A-F.

In the BASE segment, it is a repeated field that is described with the TUCNT field. Each entry contains the RACLINK status fields used for automatic command redirection. The corresponding target user is described in the TUKEY field. When output, this field contains the following subfields:

Table 405. TUDATA output - fields and descriptions

Field	Values	Meaning
Type	Master Peer Slave	Link type Authorized users can change the value in this field interactively in the RACLINK section of the User Profile detail display panel. See"User profile detail display" on page 92.
Stat	Err Pend (blank)	Link status (error, pending approval, or approved)
Pwd	Sync (blank)	Password synchronization flag. Authorized users can change the value in this field interactively from the ISPF User Profile detail display. See "User profile detail display" on page 92.
Defined	Time stamp	Time link was defined
Approved	Time stamp	Time link was approved
Creator	Userid	User that created link

See also the RACLINK field.

TUKEY

This field is found in user profile in the BASE segment. It is a repeated field that is described with the TUCNT field. Each entry contains a target userid for automatic command redirection. The corresponding RACLINK flags are described in the TUDATA field.

TUNIT

This field is found in user profiles and is part of the TSO segment. It indicates the user's default unit name for data set allocations.

TUPT

This field is found in user profiles and is part of the TSO segment. It can only be used for output. It contains data from the UPT control block, which describes the user's profile settings.

This field cannot be set using the normal RACF command; it can be set using the CKGRACF FIELD command.

TVTOC

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 2 in the RESFLG field found in TAPEVOL BASE segments. It indicates profiles with a TVTOC. It can be specified as an attribute, e.g., SELECT TVTOC. Its opposite for the purpose of SELECT/EXCLUDE processing is NOTVTOC. See also the RESFLG field.

TVTOCCNT

This field is found in GENERAL profiles and indicates the number of TVTOC entries. The entries are listed in the TVTOCSEQ, TVTOCCRD, TVTOCIND, TVTOCDSN, TVTOCVOL, and TVTOCRDS fields.

TVTOCCRD

This field is found in GENERAL profiles and indicates the creation date of a tape data set. It is a repeated field that can be combined with the TVTOCSEQ, TVTOCIND, TVTOCDSN, TVTOCVOL, and TVTOCRDS fields. The number of entries listed is in the TVTOCCNT field.

TVTOCDSN

This field is found in GENERAL profiles and indicates the RACF internal name of a tape data set. It is a repeated field that can be combined with the TVTOCCRD, TVTOCIND, TVTOCSEQ, TVTOCVOL, and TVTOCRDS fields. The number of entries listed is in the TVTOCCNT field.

TVTOCIND

This field is found in GENERAL profiles and indicates whether a discrete data set profile exists. It is a repeated field that can be combined with the TVTOCCRD, TVTOCSEQ, TVTOCDSN, TVTOCVOL, and TVTOCRDS fields. The number of entries listed is in the TVTOCCNT field.

TVTOCRDS

This field is found in GENERAL profiles and indicates the name used when creating the tape data set. It is a repeated field that can be combined with the TVTOCCRD, TVTOCIND, TVTOCSEQ, TVTOCDSN, and TVTOCVOL fields. The number of entries listed is in the TVTOCCNT field.

TVTOCSEQ

This field is found in GENERAL profiles and indicates the file sequence number of a tape data set. It is a repeated field that can be combined with the TVTOCCRD, TVTOCIND, TVTOCDSN, TVTOCVOL, and TVTOCRDS fields. The number of entries listed is in the TVTOCCNT field.

TVTOCVOL

This field is found in GENERAL profiles and indicates the volumes on which a tape data set resides. It is a repeated field that can be combined with the TVTOCCRD, TVTOCIND, TVTOCSEQ, TVTOCDSN, and TVTOCRDS fields. The number of entries listed is in the TVTOCCNT field.

UACC, UNIVACS

The Universal Access Authority of a profile. This field is found in GROUP, DATASET, and GENERAL profile types. For DATASET profiles, UNIVACS is an alias. See also the CGUACC field.

For group profiles, the UACC is NONE for all groups but VSAMDSET, where it is set to CREATE. This indicates that all users, even if they are not connected to the VSAMDSET group, are permitted to create VSAMDSET data sets.

The DATASET and GENERAL profiles can have any of the following UACC values:

- ALTER
- CONTROL
- UPDATE
- READ
- EXECUTE
- NONE

For the general resource class DIGTCERT this field has a different function. It indicates whether the digital certificate represented by the DIGTCERT profile is to be trusted (used for access). For this class the possible values are TRUST and NOTRUST.

The access given through UACC applies to all `userids`, even if they are undefined to RACF. For access given to all defined users, see `IDSTAR`.

UAUDIT

This field is found in USER BASE segments. It indicates whether the user is being audited. It can be specified as an attribute, e.g., SELECT UAUDIT. Its opposite for the purpose of SELECT/EXCLUDE processing is NOUAUDIT.

UID

This field is found in user profiles and is part of the OMVS segment. It indicates the numerical userid used for z/OS UNIX. When the `overtype` option is active, you can suffix the number with an S (e.g. 1001S), so the SHARED command keyword is added. You can also specify AUTO, which results in addition of the AUTOUID command keyword. The SHARED and AUTOUID command keywords are available in z/OS 1.4. or with APAR OW52135.

UNAME

This field is found in user profiles and is part of the NDS segment. It indicates the NDS user name. Care must be taken to ensure that this field has a unique value for each user.

UNIT

This is an alias of DEVTYPX field.

UNIVACS

This is an alias of UACC. See "UACC" on page 1204.

UNIVERSAL

This field is an alias of the UNVFLG field found in GROUP BASE segments. It indicates whether the group has the universal attribute, for example, that more than 5957 users can be connected to it. It can be specified as an attribute, e.g., SELECT UNIVERSAL. Its opposite for the purpose of SELECT/EXCLUDE processing is NOUNIVERSAL.

UNVFLG

This field is present on the group profile and is a flag byte indicating whether the group has the universal attribute, for example, more than 5957 users can be connected to it, unless they have special connect attributes. See also the UNIVERSAL and NOUNIVERSAL fields.

USEMAP

This field is found in the ICTX segment of IRR.ICTX.DEFAULTS.** profiles in the LDAPBIND general resource class. It specifies whether the Identity Context Extension (ICTX) stores an identity mapping to a local z/OS user ID when provided by the application. This field supports the `overtype` option which permits authorized users to change the value from an ISPF panel.

USER2ACS

RACF user or group id of a conditional access list entry. This is a repeated field that can be combined with the PACSCNT, PROGACS, PROGRAM, and ACL2VAR fields. Found in DATASET profiles. The number of conditional access

list entries is contained in the ACL2CNT field. The ACL combination field is the easiest way to display normal and conditional access list entries.

USERACS

This field contains the access level of an access list entry. This is a repeated field that can be combined with USERID, ACSCNT. Found in GROUP, DATASET, and GENERAL profiles. The ACLCNT field contains the number of entries.

Group profiles can have any of the following USERACS values:

- JOIN
- CONNECT
- CREATE
- USE

DATASET and general resource profiles can have any of the following USERACS values: ALTER, CONTROL, UPDATE, READ, EXECUTE, NONE.

The ACL and CONNECT combination fields are the easiest way to display this information in combination with the related fields.

USERDATA

Variable defined in C2RXDEF1 that is equivalent to USR, except that it excludes entries in use by the CKGRACF component of zSecure, queued commands, schedules, and multiple authority settings for example. See USR for subselect processing. See CKGAUTH, CKGEVENTS, CKGOTHER, CMDSEXEC, CMDSINACT, and CMDSPEND for the various CKGRACF entries.

USERDS

This is an alias of USERDSN (see "USERDSN").

USERDSN, USERDS

This field can only be used for SELECT/EXCLUDE processing. It is the complement of the FLAG1 field found in DATASET BASE segments. It indicates whether the profile covers user data sets, for example whether the high-level qualifier is a user id. It can be specified as an attribute, for example, SELECT USERDSN. Its opposite is GROUPDSN.

USERID

RACF user or group id of an access list entry. This is a repeated field of 8 characters that can be combined with USERACS, ACSCNT. Found in GROUP, DATASET, and GENERAL profiles. The ACLCNT fields lists the number of entries.

Warning: If you use this field with the USERACS field to display an access list, do *not* sort the USERID field, since the sort order of the USERACS is not changed accordingly. To display a sorted access list, use the ACL field instead.

USERNL1

This field is found in user profiles and is part of the LANGUAGE segment. It contains a 3-character code indicating the user's primary language.

USERNL2

This field is found in user profiles and is part of the LANGUAGE segment. It contains a 3-character code indicating the user's secondary language. See the USERNL1 field.

USR

The USR field is a rather special case in Security zSecure, somewhat like the ACL field. The DEFINE SUBSELECT command can be used to select only specific entries for output. See “Subselect clauses” on page 755. To select on specific combinations of values per repeat group entry, the SELECT USR(...) command can be used. See “SELECT USR(...)” on page 892.

To print just the USRDATA portion the USRDATA format can be used. See “Specifying syntax for RACF command input” on page 810.

Because entries with a `USRNM` starting with `CNG` are used for special purposes in Security zSecure, it is common to display only the other `USR` entries on many panels. See the `USERDATA` description.

As an example, to just print the USRDATA portion of the non-CNG entries one could code `userdata(usrdata,"Userdata")` in a query.

The USR field The USR field is a combination of the USRNM, USRFLG, and USRDATA fields provided by Security zSecure (the fields making up the USR field are also supported individually). Using the USR combination field instead of the individual fields has the following advantages:

- In ISPF, action characters can be used to generate CKGRACF commands to alter, copy, or delete the user fields in a profile.
- The entries used by CKGRACF are displayed in an appropriate format.
- The DEFINE command can be used to define a *subselection* of the USR field; this can be used to display only the repeat-group entries that are of interest. See “DEFINE” on page 750 for more details on subselection.

As described in the preceding paragraphs, each USR field repeat-group entry contains a USRNM field, a USRFLG field, and a USRDATA field. The USRNM field length is 8 characters long, is used as an *index*; the variable-length USRDATA field is used as the *contents*.

Security zSecure treats each USR field repeat-group entry according to its USRNM index value. All entries with an USRNM-value starting with *CNG* are treated specially. These values are reserved for use by Security zSecure. All other entries are considered installation-defined. In restricted mode, Security zSecure only grants access to those installation-defined entries to which the user is also authorized by CKGRACF. Authorization is granted using the CKGRACF profiles. See “Auditing CKGRACF” on page 371.

When the USR field is displayed, installation-defined entries are displayed in the format `USRNM USRFLG USRDATA'`. Security zSecure reserved entries are displayed in an appropriate format.

Use by Security zSecure

The CKGRACF authorized component of Security zSecure stores various types of information in the USR field of user profiles. When the USR field is displayed, these are printed in an appropriate format. This section describes the types of information stored, and the meaning of the output.

Security zSecure stores the following types of information in the USR field:

Multiple-authority settings
The multiple-authority setting determines the number of administrators required to process a CKGRACF USER command. This value is also available as the CKGMULTI field.

Default passwords
A default password is the password used by the CKGRACF

USER PWRESET and USER PWSET DEFAULT commands. Note that the default password itself cannot be displayed; its presence and the audit trail can be displayed.

Queued commands
When a user is subject to multiple-authority, a command is *queued* in the user profile until the appropriate administrators have approved (or denied) its execution. The USR field displays the queued command, a short indication of its current status, and the administrators' actions so far. The status of the queued command is also available as the CKGSTATUS field.

Scheduled revoke/resume actions
A user can be subject to multiple independent revoke/resume *schedules*, each containing revoke and resume *actions*. Each such action is stored in a USR repeat-group entry. The USR field displays the schedule name, the revoke/resume date, and the audit trail. The schedule name is also available as the CKGSCHEDULE field.

Figure 516 shows sample output of the USR field.

```
Authority setting TRIPLE set by R##PROB at 17 Feb 1994 22:07
Default password set by R##PROB at 17 Feb 1994 22:07
Queued command (R): USER CRM###3 PWDEFAULT PASSWORD;
   request by C###ROB at  4 Mar 1994 15:38
Scheduled event: Schedule 'FIRED' disable  1 Jan 1995;
   set by R##PROB at 28 Feb 1994 20:00
DBTEST   00 Installation-defined data
```

Figure 516. Sample USR fields

In the sample output, the first four entries are defined by zSecure; the last entry is installation-defined with index DBTEST. The (*R*) in the queued command indicates the current status is *request*. For a full list, see the description of the CKGSTATUS field in "SELECT and EXCLUDE" on page 884.

Action characters for the USR field

When the USR field is used in an ISPF display, action characters can be used to generate CKGRACF commands to alter, delete, or copy the USR entries. See the ISPF reference (Chapter 1, "Introduction," on page 1) for a basic description of action characters. The action characters that are permitted and the commands that are generated are dependent on the USRNM index value of the USR field. Table 406 lists the available action characters and associated action. More information about the actions is provided in the paragraphs following the table.

Table 406. Action characters and effect

Action character	Action
A	Approve a queued command
C	Create a copy of the USR entry
D	Delete a USR entry/Deny a queued command
H	Hold a queued command
I	Insert a new (blank) USR entry of the same type/index
R	Create a copy of the USR entry using ISPF panels
S	Select a USR entry for more detailed information

The action characters available are dependent on the type of USR entry:

Installation-defined USR entries
The C, D, I, and R action characters can be used with installation-defined USR entries. These commands generate a CKGRACF USRDATA command. The difference between the C and R action characters is that R prompts with an ISPF panel first, and C generates the command immediately.

Scheduled actions
The C, D, I, R, and S action characters can be used for scheduled USR actions. S displays the action in more detail. All other action characters generate a CKGRACF USER SCHEDULE command.

Queued commands
The action characters in the preceding table can be used for queued commands. The S action displays the command in more detail, including the audit trail. The A, H, and D actions approve, hold, or deny the queued command. When entered, these actions generate a CKGRACF USER command with the appropriate action. The C, I, and R actions create a new CKGRACF USER command to be requested. C immediately generates a command, I prompts with a blank ISPF panel, and R prompts with a filled-in ISPF panel.

Multiple-authority and default-password entries
No action characters can be used with multiple-authority and default-password entries.

Alternative fields to display USR data

To select profiles with USR fields, or sub-select USR repeat-group entries, a number of fields is derived from the USR field. These fields have names starting with CKG, and are described in preceding paragraphs. Beside those fields, the following fields can also be used for profile selection:

- The USRCNT field contains the number of USR entries in a profile. If the USRCNT field is zero, no USR entries can be found. A useful selection can be SELECT USRCNT>0.
- The USRNM field, which contains the index of the USR field, can be used to select profiles with relevant entries. If your installation uses the USR field with index values DB2PROJ and CICSPROJ, and you want to select those profiles with DB2PROJ entries, use SELECT USRNM=DB2PROJ. Note that the USR field still displays *all* entries in the selected profile, unless a sub-selection is used.
- The USRDATA field, which contains the contents of the USR field, can be used to select profiles with relevant contents. Because this is a variable-length field, we advise you to use the *substring scan* operator (`=:`) to search for profiles with relevant entries. If you want to find all profiles with USR fields that contain the word 'OKAYED', use SELECT USRDATA=:OKAYED. Note that the USR field still displays *all* entries in the selected profile, unless a sub-selection is used.

IBM Security zSecure Admin-specific information derived from the USR field
The following table lists the fields that describe zSecure Admin-specific information derived from the USR field. All of these fields can be used for output and profile selection. In the current version of zSecure, the date fields cannot be used for USR subselection. The **Repeated** column indicates whether the field is repeated more than once per profile. For more information, see the description of the individual fields in this section.

Table 407. IBM Security zSecure Admin-specific information derived from the USR field

Field	Type	Sub-select	Repeated	Meaning
CKGAUTHOR	Text	Yes	Yes	User who requested a queued command. Repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.
CKGCHGDATE	Date	No	Yes	Date a queued command was last changed. Repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.
CKGEXPIRY	Date	No	No	First date on which any of the queued commands expires. (Each queued command has an expire date; the earliest is taken.) Undefined if the profile does not contain queued commands.
CKGMULTI	Text	Yes	No	Multiple-authority setting.
CKGREFRESH	Date	No	No	Date after which a CKGRACF REFRESH command is required; undefined if the profile does not contain scheduled revoke/resume actions or queued commands.

Table 407. IBM Security zSecure Admin-specific information derived from the USR field (continued)

Field	Type	Sub-select	Repeated	Meaning
CKGREQUEST	Date	No	Yes	Date a queued command was requested. Repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.
CKGSCHEDULE CKGSCHED	Text	Yes	Yes	Schedule name of a scheduled revoke/resume action. Repeated for each scheduled action stored in the profile; undefined if the profile does not contain scheduled actions.
CKGSTATUS	Text	Yes	Yes	Current status of a queued command. Repeated for each queued command stored in the profile; undefined if the profile does not contain queued commands.

USRCNT

The USRCNT field is found in all profile types and describes the number of user fields. These fields are installation-reserved and are used by CKGRACF and third-party software packages. Each user field contains a USRNM index field, a USRFLG flag field, and a USRDATA contents field. The field is also available as the USR combination field.

USRDATA

The USRDATA field is found in all profile types and contains the contents part of the 'user fields' repeat group. See also the USR and USRCNT fields.

USRFLG

The USRFLG field is found in all profile types and contains the flag part of the 'user fields' repeat group. See also the USR and USRCNT fields.

USRNM

The USRNM field is found in all profile types and contains the index part of the 'user fields' repeat group. See also the USR and USRCNT fields.

UUID

This field is found on the DCE segment of the user profile. It contains the universal unique identifier of the principal. The UUID is exactly 36 characters, in the format *nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn* where n is any hexadecimal digit.

VERSION

Profile/template version number.

VOL

This is an alias of VOLSER (see "VOLSER").

VOLCNT

For DATASET and GENERAL profiles, this field specifies the number of volumes containing the tape data set. The volume serials are listed in the VOLSER field.

VOLSER, VOLUME, VOL

For DATASET and general resource profiles, this repeated field lists the volume serials of the volumes containing the (tape) data set. The number of volume serials is listed in the VOLCNT field.

The VOL field name can only be used for SELECT/EXCLUDE processing.

VOLUME

This is an alias of VOLSER (see "VOLSER").

VSAM

This field can only be used for SELECT/EXCLUDE processing. It corresponds to bit 0 in the DSTYPE field found in DATASET BASE segments. It indicates whether the profile is a VSAM data set profile. It can be specified as an attribute, e.g., SELECT VSAM. Its opposite for the purpose of SELECT/EXCLUDE processing is NONVSAM. See also the DSTYPE field.

WAACCNT

This field is found in user profiles and is part of the WORKATTR segment. It indicates the account number for APPC/MVS processing.

WAADDR1

This field is found in user profiles and is part of the WORKATTR segment. It indicates SYSOUT delivery address line 1.

WAADDR2

This field is found in user profiles and is part of the WORKATTR segment. It indicates SYSOUT delivery address line 2.

WAADDR3

This field is found in user profiles and is part of the WORKATTR segment. It indicates SYSOUT delivery address line 3.

WAADDR4

This field is found in user profiles and is part of the WORKATTR segment. It indicates SYSOUT delivery address line.

WABLDG

This field is found in user profiles and is part of the WORKATTR segment. It indicates the building for delivery.

WADEPT

This field is found in user profiles and is part of the WORKATTR segment. It indicates the department for delivery.

WANAME

This field is found in user profiles and is part of the WORKATTR segment. It indicates the user name for SYSOUT delivery.

WARN

This is an alias of WARNING (see "WARNING").

WARNING, WARN

This field is found in the BASE segment of DATASET and GENERAL profiles and indicates whether the data set or resource has the WARNING attribute, which indicates whether access is granted even if the access level requested is higher than the one permitted by other profile settings. This is a non-standard field because bit 7, not bit 0, is used. The alias WARN can only be used for SELECT/EXCLUDE processing. It can be specified as an attribute, SELECT WARNING for example. Its opposite for the purpose of SELECT/EXCLUDE processing is NOWARNING.

WAROOM

This field is found in user profiles and is part of the WORKATTR segment. It indicates the room for delivery.

WORKATTR

This field can only be used for SELECT/EXCLUDE processing. It selects WORKATTR segments.

X509REGISTRY, X509REG

This field is found in the EIM segment of LDAPBIND and FACILITY class general resource profiles. On the IRR.PROXY.DEFAULTS profile in the FACILITY class it specifies the name of the X.509 registry in the EIM domain that the system is configured to use. On other profiles it is ignored. This field supports the `overtype` option.

XRFSOFF

This field is found in user profiles and is part of the CICS segment. It is a flag field indicating whether CICS is to sign-off the operator following an XRF takeover.

RACF_ACCESS: Connects and permits

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The `RACF_ACCESS NEWLIST (NEWLIST TYPE=RACF_ACCESS)` provides information about the permits and connects used for RACF access. The input data for this `NEWLIST` type can be both the RACF database records and the Access Monitor summary

data sets which consolidate the actual access events logged over a given time interval. Alternatively, you can use the SIMULATE RACF_ACCESS command to limit the input to the RACF database records.

If you use both the RACF database and the Access Monitor summary data, the report provides information on actual permits and connect use.

If you use the RACF_ACCESS NEWLIST in combination with the SIMULATE_RACF_ACCESS option, the report provides information on the permits and connects allowed based on the RACF database profile definitions. The output is an exploded view of all permits and connects defined in the RACF database, including the effect of RACLIST merge processing.

A record in RACF_ACCESS NEWLIST output can contain any of the following types of access information:

- A permit for a profile or profile member.
- A connect for a profile or profile member.
- A group authority for a profile or profile member.

Grouping profile members are only present as separate records for RACLISTed grouping classes,

For SETROPTS or GLOBAL=YES RACLIST-ed classes, permits per member profile or grouping profile member might be present twice because the RACLIST merge result is also returned for records that have the flag RACLIST_MERGE set on.

Access counts for each access event are increased based on the following rules:

1. If SIMULATE RACF_ACCESS is not used, access events found in Access Monitor records saved in the Access Monitor summary data are counted under the profile implied by the access summary records as long as the profile key is still present in the RACF database. If a profile key is present in the access summary data but is no longer present in the specified RACF input source, the access is counted against a missing profile. In the RACF_ACCESS NEWLIST output, these types of access are listed as proftype=missing.
2. If SIMULATE RACF_ACCESS is specified, you can observe what the recorded RACF access decisions would have been, based on the specified RACF input source.

Important:

If you run a NEWLIST type=RACF_ACCESS command concurrently with a NEWLIST type=ACCESS command, the SIMULATE specification for NEWLIST TYPE=RACF_ACCESS takes precedence over the use of SIM_* fields in the NEWLIST TYPE==ACCESS. If you specify NEWLIST TYPE=RACF_ACCESS with the SIMULATE RACF_ACCESS setting, the SIM_* fields are present. If you run NEWLIST TYPE=RACF_ACCESS without the SIMULATE RACF_ACCESS setting, all SIM_* fields in the NEWLIST TYPE=ACCESS is reported as missing. For more information on the ACCESS NEWLIST type, see "ACCESS: Access Monitor Records" on page 953.

Field descriptions

The RACF_ACCESS NEWLIST provides the following fields for reporting.

ACCESS

Indicates the type of access. The following types are reported:

- ACL access for a permit.

- The connect authority for a connect.
- QUALOWN for access authority through a data set High-level qualifier.

The default field width is 9 characters.

ACCESS_COUNT_SUCC

Count of successful accesses as counted for this entry. Successful access is counted for all possible ways the user has access to the resource because the system does not determine which method is actually used by RACF. The maximum count is 2**32-1. When the maximum count has been reached, the count is not increased even if additional access events are found in the access records.

Note: This field is only supported if zSecure Admin is installed and active. In environments that only have zSecure Audit, the fields are shown as missing (blank).

ACCESS_COUNT_UNK

Count of accesses that cannot be explained by this access record entry. For example, an unknown access can be a result of an access summary record that shows successful access events that are higher than the permit access level on a user permit, or that shows a violation where the current RACF database indicates that the access permit level should have resulted in access being granted. The number has a ceiling of 65535. When the maximum count has been reached, the count is not increased even if additional unknown access events are found in the access records.

Note: This field is only supported if zSecure Admin is installed and active. In environments that only have zSecure Audit, the fields are shown as missing (blank).

ACCESS_COUNT_VIO

Count of violations that this access record entry might have caused. The number has a ceiling of 65535. When the maximum count has been reached, the count is not increased even if additional unknown access events are found in the access records.

Note: This field is only supported if zSecure Admin is installed and active. In environments that only have zSecure Audit, the fields are shown as missing (blank).

ACCESS_FIRSTUSE

The Access Monitor data collection only tracks `ACCESS_LASTUSE`. For example, if a particular access specification is used five times a day, the daily consolidation access summary file shows the last time the access specification was used during that day. If the current `RACF_ACCESS` report uses multiple daily consolidation files, the last use data for each individual daily consolidation file is the `ACCESS_LASTUSE` value recorded for each day. The `ACCESS_FIRSTUSE` field stores the value of the earliest occurrence of the `ACCESS_LASTUSE` value in all the consolidation files.

If the current `RACF_ACCESS` report uses a single Access Monitor summary file, the `ACCESS_FIRSTUSE` value is the same as the `ACCESS_LASTUSE` value in the summary file.

ACCESS_INTENT_MAX_SUC

Indicates the highest allowed access intent found in the access summary. For example, on an UPDATE permit record where the user read data, the field value is READ.

ACCESS_INTENT_MIN_VIO

Shows the lowest access violation level found in the access summary.

ACCESS_LASTUSE

Shows the date and time of last use in TOD clock format.

ACCESS_REDUCED

Flag field that indicates whether the access level granted to ID is less than the access granted using any of the GROUPS that ID is a member of, the access granted to ID(*), or the UACC.

If ID is a group, ACCESS_REDUCED=YES when the access granted by ID(*) or by UACC is higher than that granted by the group.

For ID(*), ACCESS_REDUCED=YES if its access is less than that granted by the UACC.

CLASS

Provides the 8-character RACF profile class for the profile listed in the PROFILE field. See "PROFILE" on page 1217.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

GENERIC

Flag field that shows if the profile is generic.

ID

The ACL ID for a permit, or a connected user ID for a GROUP profile, or one of the special values listed in Table 408.

Table 408. RECORD Types for NEWLIST TYPE=ACCESS

Value	Description
-UACC-	Reflects the Universal Access attribute which means that even undefined users can access the record.
- any -	Reflects access provided through the global access table which means that even undefined users can access the record.
-other-	Reflects the access level for a missing profile to count accesses.
-error-	Unexpected condition - low priority program defect.

MEMBER_CLASS

For a grouping profile member, this field provides the member class.

For grouping class profile records, a single grouping class profile is represented by multiple RACF_ACCESS records: One record describes the grouping profile itself. The remaining records describe the members. The MEMBER_CLASS for the grouping profile record is the name of the grouping class. For the multiple records describing the members, the MEMBER_CLASS is the name of the class that is linked to the grouping class (the member class).

For a non-grouping class profile the value of MEMBER_CLASS is the same as that of CLASS.

MEMBER_KEY

Shows the member key for a grouping profile member.

For grouping class profile records, a single grouping class profile is represented by multiple records. One record describes the grouping profile itself. The other records describe the members. The MEMBER_KEY for the grouping profile record is the same as the profile key in the PROFILE field. The MEMBER_KEY for the member records contains the member name.

For non-grouping class profile records, MEMBER_KEY always has the same value as the PROFILE field.

The MEMBER_KEY field represents the member key in human readable form which means that the generic member keys are sorted alphabetically and cannot be sorted by generic search order.

MERGED_ACCESS_REDUCED

Flag field that indicates if the access level granted to ID is less than that granted using any of the less specific access list entries in the profiles used during merge of grouping and member profiles. For example, if ID is a userid with READ and another merged grouping class profile specifies ID(*) with UPDATE, the access level READ is reduced from what the userid would have if access READ was not specified.

MERGED_ACCESS_REDUCED is similar to ACCESS_REDUCED except that the access specifications used to determine the value of MERGED_ACCESS_REDUCED can be taken from different profiles that are merged during the RACF RACLIST process. For the ACCESS_REDUCED field, the value is determined by access specifications for the same profile.

This field is missing for non-grouping resource classes and for records with RACLIST_MERGE=YES.

PROFILE

The PROFILE field provides the profile key in human readable form. Because the value is human readable, the RACF_ACCESS NEWLIST type does not allow you to sort the generic profiles by generic search order. The default width for this field is 44, the maximum length is 246.

For the profile class, see "CLASS" on page 1216.

PROFTYPE

Shows the profile type. Table 409 lists the available types.

Table 409. Profile Types for NEWLIST TYPE=RACF_ACCESS

Profile Type	Description
connect	Connect record.
DISCRETE	Discrete general resource profile record.

Table 409. Profile Types for NEWLIST TYPE=RACF_ACCESS (continued)

Profile Type	Description
GENERIC	Generic data set or general resource profile record.
GLOBAL	Global access table entry record.
GROUPING	Member in a grouping profile record.
missing	Indicates that a profile key is present in the access summary data but the profile key is no longer present in the specified RACF database input source.
MODEL	Model profile record.
NONVSAM	Discrete non-VSAM DATASET profile record.
TAPEDSN	Discrete tape data set profile record.
VSAM	Discrete VSAM profile.

QUALIFIED_RESOURCE

This field concatenates values in the RESOURCE_LOCATION and RESOURCE fields (separated by a colon) and shows which transaction name is defined in which region. It has a default length of 64 characters and a maximum length of 282 characters. An example value is IPO1.CICS.CICSTS41.TRN:CEMT. The format is as follows:

system.subsys-type.subsys-identification.restype:<resource>

Note: The maximum number of entries is the product of the number of entries in these two fields. If there are 10 resource names and 20 resource locations, the QUALIFIED_RESOURCE field might contain as many as 200 entries.

RACLIST_MERGE

Flag field that indicates whether the record is part of the RACLIST merge result. When the flag value is `YES`, the record represents the in-storage profile built during the RACF RACLIST process. If you only want to see basic database permits and connects, filter the report results using `RACLIST_MERGE=NO`.

Note:
The RACLIST process is used by RACF either during the SETROPTS RACLIST command processing or when an application that starts `RACROUTE REQUEST=LIST,GLOBAL=YES.`

RESOURCE

Select or show the names of resources that match the permit. The RESOURCE field shows only those resources that are effectively protected by the permit to the PROFILE. For RACLISTed resource classes, the RACLIST merge process can result in overruling the access specified in one grouping class profile by a (higher) access specified in another grouping or member class profile. If access is overruled, the RESOURCE field for the PROFILE is empty. For other IDs, an access overrule might not apply and the RESOURCE field includes all applicable resources.

You can also automatically include which sensitive resources or data sets are covered by each profile using the command `REPORT RESOURCE` or `REPORT DATASET`, respectively. To include both types, specify the command `REPORT RESOURCE DATASET`. Before using these options, consider the amount of output that will be generated, especially when including data sets. Without any further

SELECT statements, these options cause a combinatorial explosion of the number of resources in the system times the number of permits in the profiles that cover them. The volume of output generated might exceed acceptable job output size at your site. You can issue the SUPPRESS AUTO_RESOURCE command to limit the report to resources for which you have issued a SIMULATE CLASS or SIMULATE RESOURCEcommand or a SIMULATE SENSITIVE command.

RESOURCE_LOCATION

Identifies the resource name environment. This repeat group field includes the RESOURCE_LOCATION field only. The default and maximum length is 35 characters. An example value with four qualifiers is IPO1.CICS.CICSTS41.DATASET. The SIMULATE command automatically generates resource names. Names can include two or four qualifiers. The *subsys-identification* and *restype* qualifiers are optional. The format is as follows:

system.subsys-type.subsys-identification.restype

If you want to see which transaction name is defined in which CICS region, use the QUALIFIED_RESOURCE field in your report instead of using the RESOURCE and RESOURCE_LOCATION fields. The RESOURCE_LOCATION repeat group produces results that are independent of the RESOURCE field even though the results might appear related if these fields appear side-by-side in a report.

VOLSER

Shows the first volume serial. This field is only present for discrete VSAM, non-VSAM, and tape DATASET profiles.

REPORT_AC1: Authorized module protection

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

The REPORT_AC1 NEWLIST (NEWLIST TYE=REPORT_AC1) only reports on the default system. The default system is set using the DEFAULT command.

This NEWLIST has been built to audit the protection of programs that run with a system-level authorization and are callable by users that do not yet have such an authorization level. Penetrating the security built into those programs usually yields total control over the operating system to a *normal* user. This makes these programs a target for hackers. For a list of the authorizations checked see the AUTH field.

A CKFREEZE file is required and must include PDS directory information for this function. This means that zSecure Collect must be run on z/OS with the proper focus. The focus will automatically be OK if you run zSecure Collect with the same entitlements as CKRCARLA. If you are analyzing a CKFREEZE file created on z/OS with different entitlements or a specific focus, you must be aware that for REPORT AC1 the focus must include at least one of AUDITRACF, AUDITACF2, or ADMINRACF. It must also be run APF authorized or non-APF authorized with PDS=YES added and sufficient access on *all* linklist and APF data set directories. When run without APF authorization, PPT information and module information where the CKFCOLL caller has no read access will be missing.

The CARLa script CKRRAC1 containing this NEWLIST type is included automatically by the REPORT AC1 command if the NEWLIST type was not yet specified in the input above the REPORT command.

Field descriptions

The REPORT_AC1 NEWLIST provides the following fields for reporting.

AUTH

This repeat group field indicates sources of authorization for the module. Table 410 provides the value and description for the authorization source type that can be reported.

Table 410. TYPE=REPORT_AC1 - AUTH parameter values for module authorization source types

Authorization source type	Description
AC=1:Bypass	RACF and password security, from the Program Property Table (PPT).
AuthCMD	Can be called as TSO authorized command.
AuthPGM	Can be called under TSO as an authorized program.
AuthTSF	Can be called as authorized through the TSO service facility.
IEAAPP00	I/O appendage that is authorized for use by non-APF users
Key=n	System key from the PPT.
RACINIT	from RACF authorized caller table ICHAUTAB
RACLIST	from ICHAUTAB.
Signed	The signed attribute bit is on in the PDSE directory entry for the module. The Signed attribute bit being on does not mean that the signature is valid or even present.
SigProb	A problem occurred when the zCollect program (CKFCOLL) attempted signature verification.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

DSN

Contains the name of the data set where the module resides or presumably was loaded from (for LPA modules). In addition, it can contain the string '*** LPA

' to indicate that it was present in the link pack area in-storage but that no corresponding load module name was found in an LPA data set. Also, it can contain the string ' module not found ***' to indicate that it was not found in the link pack area in-storage nor in any PDS.

HIDDEN_LINKLIST

This is a flag that indicates that this module is hidden from view in the link list (for example, in the concatenation, a different module will be loaded).

HIDDEN_LPALIST

Flag field that indicates if this module is hidden from view in the LPA list. That is, in the concatenation, a different module is loaded.

LINKLIST

Concatenation number of the module's data set in the current link list set. It might be empty to indicate the module is not in the current link list set.

LPALIST

Concatenation number of the module's data set in the LPA list. It might be empty to indicate the module is not in the LPA list.

LPA_TYPE

One-character field that can have one of the following values: `F` for Fixed Link Pack Area, `M` for Modified Link Pack Area, `P` for Pageable Link Pack Area, or blank if the module is not in the LPA

MEMBER

Returns the member name that contains the load module for the program, or the major name of a module in-storage where the actual member could not be found in a PDS directory.

MODULE

Returns the name of a program entry point that is available in the system. It is not necessarily equal to the member name, a load module can contain more than one program entry point.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PROGRAM

Returns the name of a RACF PROGRAM profile if it covers the program when loaded from a data set. Note that an LPA module is not subject to program control in its already loaded form, although it is considered to be a 'controlled' program anyway.

PROGRAM_TYPE

Since z/OS V1.4, RACF can run in Enhanced program security mode. In this mode, a program can be defined as MAIN or BASIC program. This field returns the type of the program.

PROFILE

Returns the name of the RACF DATASET profile that protects the load library where the load module member resides.

STAMP

Returns the unload time stamp of the security database.

SYSTEM

Returns the name of the system this report pertains to. The REPORT_AC1 NEWLIST describes only one system, the default system. It can be changed by the DEFAULT command.

UACC

For a RACF system, this field contains the consolidated universal access for the program. To arrive at this universal access, a number of questions are first answered internally to get a full picture of the protection. These are:

1. (RACF) Do the DATASET profiles covering the APF data sets containing the module have UACC(NONE)?
2. (RACF) Is the module covered by a PROGRAM profile in all data sets?
3. (RACF) Does the PROGRAM profile have UACC(NONE)?
4. Is one of the APF data sets part of the linklist concatenation?
5. Which (APF or non-APF) data set is the first in the linklist concatenation to contain the module?
6. Is the module present in LPA?
7. Is the module present in MLPA?
8. (RACF) Is the data set covered by a global access table entry with READ or higher?
9. (RACF) Is the data set profile in warning mode?

The program determines the answers to these questions, and deduces the resulting universal access to the module, showing EXECUTE or higher if anybody (not explicitly denied access) can execute it. This column can display some special access levels not normally defined by the security package. The following table shows all possible UACC levels.

Table 411. UACC levels and descriptions

UACC level	Description
ALTER	The data set UACC allows ALTER to any task or user in the system. This is a major leak.
AD-UPD-NX	The data set UACC allows ALTER to any task or user in the system, but the program is not directly executable because the PROGRAM profile UACC is NONE. This is a major leak.
UPDATE	The data set UACC allows UPDATE to any task or user in the system. This is a major leak.
UPD-NX	The data set UACC allows UPDATE to any task or user in the system, but the program is not directly executable because the PROGRAM profile UACC is NONE. This is a major leak.
READ	The data set UACC allows READ to any task or user in the system. This makes it vulnerable to analysis by a hacker.
READLPA	The data set UACC does not allow READ, but module can be read in LPA. This makes it vulnerable to analysis by a hacker.

Table 411. UACC levels and descriptions (continued)

UACC level	Description
LOADEXE	The data set UACC does not allow READ, but the module can be executed, and it can be read by issuing LOAD (this requires that you know the module name).
EXECUTE	The data set UACC does not allow READ, and the module can only be executed in a controlled environment.
COPY	The module can be read, but it cannot be executed. If its operation does not depend on APF or library residence (PADS), anyone can access its functionality by copying it to his own load library.
HIDDEN	The module UACC is NONE, because it is hidden by a similar-named module concatenated in front of the LPA or linklist concatenation.
NONE	The module UACC is NONE. It is only available to specifically authorized users or groups.

Note: Since z/OS V1.4, modules protected by the `*` or `**` `PROGRAM` profile and read from `SYS1.LINKLIB` can always be executed. In effect, those `PROGRAM` profiles have at least `UACC(READ)`.

VOLSER

Contains the volume serial where the data set indicated in DSN resides.

REPORT_NONDEFAULT: RACF profiles changed from default

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

For group data sets, this lists 'out-of-group' access as discussed in “REPORT_OUTOFGROUP: RACF profiles accessible outside group” on page 1226 as well as 'out-of-group' access where the 1st qualifier is another group than the OWNER. However, userids in the access list are not checked for connects, but always marked as non-default, unless they are equal to either the OWNER or the 1st qualifier (an explicit PERMIT command must have been used to create this situation, and in this sense they are non-default).

In addition, user data set profiles are listed where other people than the owner are in the access list or in the OWNER field (or UACC not equal to NONE). The profiles can be augmented with the actual data sets they cover by making sure the REPORT DATASETS option is present.

The CARLa script CKRRNDEF containing this NEWLIST type is included automatically by the REPORT NONDEFAULT command if the NEWLIST type was not yet specified in the input above the REPORT command.

Field descriptions

The `REPORT_NONDEFAULT NEWLIST` provides the following fields for reporting.

ACCESS

Repeat group field that returns the access level column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ID

Repeat group field that returns the user or group ID column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

KEY

Repeat group field that returns the RACF profile name followed by the data set names that it covers. The data set names are only present when the `REPORT DATASETS` parameter has been requested.

MARK

Repeat group field that returns the annotation column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM. This field contains an arrow '->' to highlight a specific access list entry that is not default.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE, NONDISPL to implement the REPORT PAGEBY= parameter.

PROFTYPE

Part of a repeat group with the KEY and VOLUME fields, this field returns the RACF profile type (GENERIC, NONVSAM, TAPE, MODEL) for the first or only line, and the data set type for subsequent lines. For a list of data set types, see "PROFTYPE" on page 1244.

PROGRAM

Repeat group field that returns the program conditional access column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

QUAL

Indicates the first qualifier of the data set profile as modified by ICHCNX00 and ICHNCV00. This value can be used to group related profiles together on separate pages.

REASON

Returns a reason why the profile is considered to be a non-default profile. There might be more reasons, but only one is spelled out. However, *all* access list entries present that are considered non-default are marked with an arrow in the field MARK. The reasons that can be present are:

Table 412. Reason field values and descriptions

Reason	Description
Conditional access	An entry in the conditional access list is always considered non-default.
Group access	The owning group or the data set's 1st qualifier group must be in the access list of a group data set profile to be considered default. In addition, the access must be either ALTER or UPDATE. ALTER is the preferred way, especially in a generic profile environment with PROTECTALL active, since data set creation is otherwise impossible. However, the RACF default set by the GRPACC attribute is UPDATE, therefore this is considered default, too. The entry will be marked with an arrow unless it is missing from the access list.
Missing access	To be considered default, access must be granted either to the first qualifier identity or to the owner, either implicitly (e.g. 1st qualifier is a userid) or explicitly (by means of an access list entry).
More than 1 group	For an access list to be considered default, it might contain only one group, either the 1st qualifier group or the owning group. Other groups are marked with an arrow.
Not owner or group	An identity in the access list is only considered default if it is the owner, or if it is a group and equal to the 1st qualifier. An undefined identity is never considered default. The identity is one of the entries marked with an arrow.
Owner access not ALTER	To be considered default, the identity owning the profile must have ALTER access to his data.
Owner not in group	The owner of a group data set profile is a user without connect to the group. Note that the notion of data set groups presupposes that ownership is a user group, not a user.
Universal access	UACC is unequal to NONE, giving access outside the group.
User not owner	The data set name starts with a userid. To be considered default, the data set profile owner must be that userid.

STAMP

Returns the unload time stamp of the RACF database. It cannot be used for SELECT and EXCLUDE processing.

UACC

Returns the universal access of the profile.

VOLSER

A repeat group field that combines with the KEY field. On the first or only line of an entry, this field shows the volume serial of the RACF profile in the KEY field. This value is only provided for discrete profiles. In the next lines it shows the volume serial where the data sets in the corresponding lines of KEY reside. The latter are only present when the REPORT DATASETS option has been requested.

REPORT_OUTOFGROUP: RACF profiles accessible outside group

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The REPORT_OUTOFGROUP NEWLIST (NEWLIST TYPE=REPORT_OUTOFGROUP results in a display of group data set profiles that have a UACC other than NONE, or an OWNER or access list entry for a user or group outside the group indicated by the first qualifier as modified by ICHCNX00 and ICHNCV00.

The report can be used by sites that have a simple RACF group structure with both user and data set profiles, to get a small report of profiles with a 'non-standard' access list, as opposed to a complete list of all profiles. This is especially useful in all-discrete environments, where typically most of the profiles have a default layout.

For sample output see "RA.3.5 OUT OF GROUP - Group data sets that can be accessed from outside the group" on page 212.

The CARLa script CKRROUTG containing this NEWLIST type is included automatically by the REPORT OUTOFGROUP command if the NEWLIST type was not yet specified in the input above the REPORT command.

Field descriptions

The REPORT_OUTOFGROUP NEWLIST provides the following fields for reporting.

ACCESS

This repeat group field returns the access level column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ID

Repeat group field that returns the user or group ID column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

KEY

Repeat group field that returns the RACF profile name followed by the data set names that it covers. The data set names are only present when the REPORT DATASETS parameter has been requested.

MARK

Repeat group field that returns the annotation column of the combined access list defined by MARK, ID, ACCESS, and PROGRAM. The field contains an arrow '->' to highlight the specific access list entry that points out of the group.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PROFTYPE

This field is part of a repeat group with the KEY and VOLUME fields. IN the first or only line in the listing, the value represents the RACF profile type (GENERIC, NONVSAM, TAPE, or MODEL). For subsequent lines, it provides the data set type. For a list of data set type see "PROFTYPE" on page 1244.

PROGRAM

Repeat group field that returns the program conditional access column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

QUAL

Field that indicates the first qualifier of the data set profile as modified by ICHCNX00 and ICHNCV00. The field can be used to group related profiles together on separate pages.

REASON

Field that indicates the first reason why a profile was included in the report. There might be more reasons, but only one is spelled out. However, all access list entries referring outside the data set 1st-qualifier group are marked with an arrow in the field MARK. Table 413 lists the possible values for the REASON field.

Table 413. REPORT_OUTOFGROUP: Reason field values and descriptions

Value	Description
Universal access	UACC is unequal to NONE, giving access outside the group.
User not in group	A user in the access list or OWNER field is not connected to the data set's 1st qualifier group. If it is a user in the access list, the user is one of the entries marked with an arrow.
Other group	A group in the access list or OWNER field was present different from the data set's 1st qualifier group. If the group is part of the access list, it is one of the entries marked with an arrow.

STAMP

Returns the unload time stamp of the RACF database. This field cannot be used for SELECT or EXCLUDE processing.

UACC

Returns the universal access of the profile. This field supports overtype.

VOLSER

Repeat group field with the KEY field that shows the volume serial of the RACF profile in the KEY field on the first or only line for an entry. The value is only listed for discrete profiles. In the next lines the volume serial where the data sets in the corresponding line of KEY reside. The latter are only present when the REPORT DATASETS option has been requested.

REPORT_PADS: Programs giving access to data sets

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The REPORT_PADS NEWLIST (NEWLIST TYPE = REPORT_PADS) is used for auditing the protection of programs that grant additional access to another data set when they are run. These programs occur in the conditional access list of some data set profile. For RACF, this type of access is known as PADS, Program Access to Data Sets (PADS). PADS programs are included in the conditional access list of some data set profile. Penetrating the security built into those programs usually yields control over some application, unless the data set is part of the Trusted Computing Base, in which case the operating system might be compromised. These programs are a potential target for hackers, although they are less tempting than the programs reported by the REPORT_AC1 NEWLIST.

This REPORT_PADS NEWLIST only reports on the default system. The default system can be set with the DEFAULT command. Using the REPORT_PADS NEWLIST requires CKFREEZE data that includes PDS directory information. This means that zSecure Collect must be run on a z/OS system that running zSecure Audit for RACF (zSecure Collect parameter settings FOCUS=AUDIT and FOCUS=RACF.

A CKFREEZE file is required and must include PDS directory information for this function. zSecure Collect must also be run APF authorized or non-APF authorized with the PDS=YES parameter added and sufficient access on *all* link list and APF data set directories. If the data collection is run without APF authorization, the data does not include PPT information and module information where the CKFCOLL caller has no read access.

The CARLa script CKRRPADS containing this NEWLIST is included automatically by the REPORT PADS command if the NEWLIST type was not yet specified in the command input that precedes the REPORT command.

Field descriptions

The REPORT_PADS NEWLIST field provides the following values.

AUTH

Repeat group field that indicates additional sources of authorization for the module (besides PADS). It can be *AC=1 Bypass* (bypass RACF and password security, from Program Property Table PPT), *Key=n* (system key, from PPT), *RACINIT* (from RACF authorized caller table ICHAUTAB), *RACLIST* (from ICHAUTAB), *AuthCMD* (can be called as TSO authorized command), *AuthPGM* (can be called under TSO as an authorized program), *AuthTSF* (can be called as authorized through the TSO service facility), and *IEAAPP00* (I/O appendage that is authorized for use by non-APF users).

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

DSN

Contains the name of the data set where the module resides or presumably was loaded from (for LPA modules). In addition, it can contain the string '*** LPA ***' to indicate that it was present in the link pack area in-storage but that no corresponding load module name was found in a LPA data set. Also, it can contain the string '*** module not found ***' to indicate that it was not found in the link pack area in-storage nor in any PDS.

HIDDEN_LINKLIST

Flag field that indicates if this module is hidden from view in the link list. That is, in the concatenation, a different module is loaded.

HIDDEN_LPALIST

Flag field that indicates if this module is hidden from view in the LPA list. That is, in the concatenation, a different module is loaded.

LINKLIST

Concatenation number of the data set for the module in the current link list set. This field might be empty to indicate the module is not in the current link list set.

LPALIST

Concatenation number of the data set for the module in the LPA list. This field might be empty to indicate the module is not in the LPA list.

LPA_TYPE

This one character field can have the following values: `F` for Fixed Link Pack Area, `M` for Modified Link Pack Area, `P` for Pageable Link Pack Area, or blank if the module is not in the LPA.

MEMBER

Returns the member name that contains the load module for the program, or the major name of a module in-storage where the actual member could not be found in a PDS directory.

MODULE

This field returns the name of a program entry point that is available in the system. It is not necessarily equal to the member name (a load module can contain more than one program entry point).

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PROGRAM

Returns the name of a RACF PROGRAM profile if it covers the program when loaded from a data set. Note that an LPA module is not subject to program control in its already loaded form, but it is considered controlled anyway.

PROGRAM_TYPE

Since z/OS V1.4, RACF can run in Enhanced program security mode. In this mode, a program can be defined as MAIN or BASIC program. This field returns the type of the program.

PROFILE

Returns the name of the DATASET profile that protects the load library where the load module member resides.

STAMP

Returns the unload time stamp of the RACF database. It cannot be used for SELECT/EXCLUDE processing.

SYSTEM

Returns the name of the system this report pertains to. The REPORT_PADS NEWLIST describes only one system, the default system. It can be changed by the DEFAULT command.

UACC

For a RACF system, this field contains the consolidated universal access for the program. To arrive at this universal access, the following questions are first answered internally to get a full picture of the protection:

1. (RACF) Do the DATASET profiles covering the APF data sets containing the module have UACC(NONE)?
2. (RACF) Is the module covered by a PROGRAM profile in all data sets?
3. (RACF) Does the PROGRAM profile have UACC(NONE)?
4. Is one of the APF data sets part of the linklist concatenation?
5. Which (APF or non-APF) data set is the first in the linklist concatenation to contain the module?
6. Is the module present in LPA?
7. Is the module present in MLPA?
8. (RACF) Is the data set covered by a global access table entry with READ or higher?
9. (RACF) Is the data set profile in warning mode?

The program determines the answers to these questions, and deduces the resulting universal access to the module, showing EXECUTE or higher if anybody (not explicitly denied access) can execute it. This column can display some special access levels not normally defined by the security package. The following table shows the whole range between NONE and UPDATE.

Table 414. REPORT_PADS: UACC level and description

UACC level	Description
UPDATE	The data set UACC allows UPDATE to any task or user in the system. This is a leak.

Table 414. REPORT_PADS: UACC level and description (continued)

UACC level	Description
READ	The data set UACC allows READ to any task or user in the system. This makes it vulnerable to analysis by a hacker.
READLPA	The data set UACC does not allow READ, but module can be read in LPA. This makes it vulnerable to analysis by a hacker.
LOADEXE	The data set UACC does not allow READ, but the module can be executed, and it can be read by issuing LOAD (this requires that you know the module name).
EXECUTE	The data set UACC does not allow READ, and the module can only be executed in a controlled environment.
COPY	The module can be read, but it cannot be executed. If its operation does not depend on APF or library residence (PADS), anyone can access its functionality by copying it to his own load library.
HIDDEN	The module UACC is NONE, because it is hidden by a similar-named module concatenated in front of the LPA or linklist concatenation.
NONE	The module UACC is NONE. It is only available to specifically authorized users or groups.

VOLSER

Contains the volume serial where the data set indicated in DSN resides.

REPORT_PROFILE: RACF profiles and data sets

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The `REPORT_PROFILE NEWLIST` is a predefined report for listing the most-used fields of profiles that you select. It is automatically included by the `REPORT PROFILES` command. In addition, you can request the names of data sets covered by the profile to be added. Contrary to the `LD DSNS` parameter in RACF, this also includes uncataloged data sets, the original data set names for backed-up discrete profiles, and single-qualifier data set names. This is requested by adding the `DATASETS` parameter to an existing `REPORT` command or by adding a `REPORT DATASETS` command after your NEWLIST requests.

The CARLa script CKRRPROF containing the `REPORT_PROFILE NEWLIST` is included automatically by the `REPORT PROFILE` command if the NEWLIST type was not yet specified in the input above the `REPORT` command.

Field descriptions

The `REPORT_PROFILE NEWLIST`

ACCESS

Repeat group field that returns the access level column of the annotated combined access list defined by ID, ACCESS, and WHEN.

AUDITF

Returns the lowest access level that results in auditing of access attempt failures. This value is empty if failure auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

AUDITLVL

A combination field that returns the values from the AUDITS and AUDITF fields. However, this field can support overtype so that authorized users can change the value. This field is not available for selection. Use AUDITS and AUDITF instead.

AUDITS

Returns the lowest access level that results in success auditing. It is empty if success auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

CLASS, C

Returns the RACF class name or entity type.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ERASE

Flag field that shows whether erase-on-scratch is active for the profile. It only shows the profile flag. To be used, the corresponding SETROPTS and HSM settings must also be on. This field supports overtype.

ID

Repeat group field that the user or group ID column of the annotated combined access list defined by ID, ACCESS, and WHEN.

KEY

This field is part of a repeat group that includes the RACF profile name followed by the data set names that it covers. The data set names are only present when the REPORT DATASETS parameter has been requested.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PROFTYPE

This field is part of a repeat group that includes the KEY, VOLUME, and the RACF profile type (GENERIC, NONVSAM, TAPE, MODEL) for the first or only line of an entry, and the data set type for subsequent lines. For a list of data set types see "PROFTYPE" on page 1244.

RESOURCE_LOCATION

Identifies the resource name environment. This field is part of a repeat group that includes the KEY, VOLSER, PROFTYPE, and SENSTYPE fields. The default and maximum length is 35 characters. An example value is IPO1.CICS.CICSTS41.DATASET. The format is as follows:

system.subsys-type.subsys-identification.restype

STAMP

Returns the unload time stamp of the RACF database. It cannot be used for SELECT/EXCLUDE processing.

UACC

Returns the universal access of the profile. This field supports overtype.

VOLSER

Repeat group field that includes the KEY value. In the report or display panel, the first or only line for an entry shows the volume serial of the RACF profile in the KEY field. This value is only provided for discrete profiles. In the subsequent lines, the volume serial is shown for the volume where the data sets in the corresponding line of the KEY are stored. The data set volume serial numbers are present only when the REPORT DATASETS option has been specified.

WHEN

Repeat group field that returns the conditional access column of the annotated combined access list defined by the ID, ACCESS, and WHEN fields. The WHEN value contains a class name and a profile name. For unconditional access list entries, this field is left blank.

REPORT_REDUNDANCY: RACF profile redundancy

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The `REPORT_REDUNDANCY NEWLIST (NEWLIST TYPE=REPORT_REDUNDANCY)` reports if data set profiles can be considered redundant and if not, the *reason* why profiles were considered non-redundant.

For a profile to be considered *redundant*, three profile properties are checked:

1. Access requirements (access list, conditional access list, and universal access).
2. Audit requirements (failure audit level, success audit level).
3. Erase-on-scratch requirement.

The first two items are simply compared to those of the most specific matching generic profile, called the *candidate* profile. They must be equal before the profile is considered redundant. However, the *erase-on-scratch* requirement is not checked if the system wide option ERASE(ALL) or NOERASE is active.

The access requirement comparison is more complicated. Simplest is the *universal access* (UACC) comparison. For a profile to be considered redundant, its UACC must either be equal to that of the candidate profile, or less than ALTER and at the same time less than or equal to the most specific matching entry of the Global Access Table (for example, a member of the DATASET profile in class GLOBAL).

The *access list* and *conditional access list* comparison takes into account group membership of userids in the list. That is, a userid in the conditional list of a redundant profile might be missing from the conditional access list of the candidate profile only, if one of the connect groups is present with the same access (and the same program name), and no connect groups are present with a higher access (and the same program name).

Note that the redundancy check does not take all fields into account; e.g. the RESOWNER and NOTIFY fields, and security categories, levels, and labels are not checked.

The NEWLIST type was primarily designed to greatly automate conversions of all-discrete environments to generic.

Unless you include select statements, the NEWLIST can list some profiles twice: once as a candidate profile, and once as a non-redundant profile.

The CARLa scripts CKRREDUN and CKRRNONR containing this NEWLIST type are included automatically by the REPORT REDUNDANT and REPORT NONREDUNDANT commands if the NEWLIST type was not yet specified in the input above the REPORT command.

Field descriptions

The `REPORT_REDUNDANCY NEWLIST` supports the following fields for reporting.

`ACCESS`

Repeat group field that returns the access level column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

`AUDITF`

Returns the lowest access level that results in auditing of access attempt failures. It is empty if failure auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

AUDITLVL

This field is a combination of the fields AUDITS and AUDITF ; contrary to these, it supports overtype . This field is not available for selection. Use AUDITS and AUDITF instead.

AUDITS

This returns the lowest access level that results in success auditing. It is empty if success auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ERASE

Flag field that shows whether erase-on-scratch is active for the profile. It only shows the profile flag. To be used, the corresponding SETROPTS and HSM settings must also be on. This field supports overtype.

ID

Repeat group field returns the user or group ID column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

KEY

A repeat group field that returns the RACF profile name followed by the data set names that it covers. The data set names are only present when the REPORT DATASETS parameter has been requested.

MARK

Repeat group field that returns the annotation column of the combined access list defined by MARK, ID, ACCESS, and PROGRAM. The field contains an arrow '->' if the corresponding access list entry makes the profile non-redundant.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

OWNER

Returns the owner of the RACF profile. This field supports overtype.

PAGEBY

Returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE, NONDISPL to implement the REPORT PAGEBY= parameter.

PROFTYPE

This field is part of a repeat group with KEY and VOLSER. For the first or only line in the listing, it provides the RACF profile type (GENERIC, NONVSAM, TAPE, MODEL). For subsequent lines, it provides the data set type. For a list of data set types see "PROFTYPE" on page 1244.

PROGRAM

Repeat group field that returns the program conditional access column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

QUAL

Contains the data set qualifier as it can have been modified by the naming convention table ICHNCV00 and naming exit ICHCNX00.

REASON

This field helps to determine the reason why the profile is included in the report. In addition, the field MARK contains arrows to point to entries in the access list (or the OWNER field) that make the profile different from the most specific matching generic. While all access list entries are considered for marking with an arrow, the REASON field returns only the first condition that caused inclusion on the report. This condition does not necessarily result in an arrow in the MARK column, and neither does an arrow need to correspond with the first reason listed.

The reasons that can appear in the redundancy report are described in Table 415.

Table 415. REPORT_PROFILE REASON field: values and descriptions

Reason	Description
- candidate -	This is a generic profile or entry in the global access table that was the most specific matching generic for one of the profiles considered non-redundant.
- redundant -	This is only present if you requested REPORT REDUNDANT. It marks all profiles that were considered redundant.
Access	The access level of a user or group in the access list of this profile was different from the access level in the access list of the candidate profile for the same identity (user or group), and it was not overruled anyway by an entry in the global access table. The entry is one of the entries marked with an arrow.
Audit	The audit requirements are different from the candidate generic profile.
Erase	The erase-on-scratch requirement is different from that of the candidate generic profile. These profile requirements are not considered if the ERASE(ALL) or NOERASE global options are active.
Extra group	The access list of this profile contains a group that is not present on the access list of the candidate generic profile. It is one of the entries marked with an arrow.

Table 415. REPORT_PROFILE REASON field: values and descriptions (continued)

Reason	Description
Missing group	The access list of this profile does not contain a group that is present in the access list of the candidate generic profile. You must look up the candidate profile access list to see which group. No arrow is present.
Missing user	The access list of this profile does not contain a userid that is present in the access list of the candidate generic profile. Nor is that userid given the same access anyway by means of one of his connects. You must look up the candidate profile access list to see which group. No arrow is present.
No generic	There is no matching generic to serve as candidate.
Undefined id	There is an extra user or group present in the access list that is not present in the access list of the candidate generic profile. However, the user or group was not defined.
Used as model	The profile is used as a model on a USER or group profile and hence not redundant.
User no connect	Might also be called Extra User. A userid is present in the access list that is not present in the access list of the candidate profile. Nor does that user have a connect to any of the groups present in the access list of the candidate generic profile. The userid will be one of the entries marked by an arrow.
User privileged	A userid is present in the access list that is given more access than the equivalent entry in the access list of the candidate profile (either the userid or the connect group giving the highest access). The userid will be one of the entries marked by an arrow. You will have to look at the candidate profile access list to find the access level involved.
User restricted	A userid is present in the access list that is given less access than the equivalent entry in the access list of the candidate profile (either the userid or the connect group giving the highest access). The userid will be one of the entries marked by an arrow. You will have to look at the candidate profile access list to find the access level involved.
Universal access	UACC is different from the candidate profile's UACC.

STAMP

Returns the unload time stamp of the RACF database. It cannot be used for SELECT/EXCLUDE processing.

UACC

Returns the universal access of the profile. This field supports overtype.

VOLSER

Repeat group field that includes the KEY and PROFTYPE values. In the report or display panel, the first or only line for an entry shows the volume serial of the RACF profile in the KEY field. This value is only provided for discrete profiles. In the subsequent lines, the volume serial is shown for the volume where the data sets in the corresponding line of the KEY are stored. The data set volume serial numbers are present only when the REPORT DATASETS option has been specified.

REPORT_SCOPE: RACF profiles and data sets in scope

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•	•		

The REPORT_SCOPE NEWLIST (NEWLIST TYPE=REPORT_SCOPE) reports the scope of a user or group. This NEWLIST shows the profiles, and optionally, the resources to which a user or group has *direct* or *indirect* access. An example of indirect access is the ability to modify a profile to give oneself direct access. To generate the report, the NEWLIST TYPE=REPORT_SCOPE statement must be followed by a REPORT command. The REPORT command must include one or more SCOPE=*id* parameters that specify the users or groups to be included in the report. To prevent inadvertent listing of all or almost all profiles and resources in the system, the system-wide *special*, *operations*, and *auditor* attributes are *not* reported. The following access types are taken into account during the reporting process:

- Access permitted by universal access and warning mode of profiles.
- Access permitted by group ownership authority (special, operations, and auditor)
- Access permitted by CREATE authority through a connect or class authorization.
- Access through the Global access table.
- Access through missing profiles.
- Access through discrete/generic DATASET profiles mismatches (in a NOPROTECTALL environment).

Access through ownership, group-special, -operations, and -auditor authority is taken into account. as well as CREATE authority through a connect or class authorization

If the NEWLIST type was not yet specified in the input preceding the REPORT command, the REPORT SCOPE= command automatically includes the CARLa script CKRRSCOP that contains this NEWLIST type.

In the ISPF interface, the REPORT_SCOPE NEWLIST can be run from option **RA.3.4**.

Field descriptions

The REPORT_SCOPE NEWLIST provides the following fields for reporting.

ACCESS

Provides the access level the ID has to the resource listed in CLASS and KEY via the path specified through VIA and WHEN. If you want to support overtype for this field, use the ACCESS_VIA_WHEN field instead of ACCESS.

See "ACCESS= level" on page 876 for an explanation of ACCESS field values.

ACCESS_VIA_WHEN

This field is a combination of the ACCESS, VIA, and WHEN fields. However, the ACCESS_VIA_WHEN field can be modified (overtypeable), while the ACCESS and VIA fields cannot be modified. The ACCESS_VIA_WHEN field cannot be used in SELECT and EXCLUDE statements. To use this information for selection criteria, use the separate ACCESS, VIA, and WHEN fields.

CLASS, C

Returns the RACF class name or entity type.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ID

Lists the user ID or group name that is used to determine the scope. This field must have been specified on a `REPORT SCOPE=`*id* command.

KEY

Repeat group that returns the RACF profile name followed by the data set names that it covers. The data set names are only present when the REPORT DATASETS parameter has been requested. See "REPORT" on page 875.

ORDER

Returns a number that when sorted corresponds to the sort order designated by the `REPORT BY=` parameter. It can be used with the modifier NONDISPL to implement the `REPORT BY=` parameter. See "REPORT" on page 875.

PAGEBY

Returns a number that increases at each page break implied by the `REPORT PAGEBY=` parameter. This value can be used with the modifiers `PAGE` and `NONDISPL` to implement the `REPORT PAGEBY=` parameter. See "REPORT" on page 875.

PROFTYPE

Part of a repeat group with the `KEY` and `VOLSER` fields. For the first or only line of an entry, this field returns the RACF profile type (*GENERIC*, *NONVSAM*, *TAPE*, *MODEL*) for the first or only line, and the data set type for subsequent lines. For a list of data set types see "PROFTYPE" on page 1244.

RESOURCE_LOCATION

Identifies the resource name environment. This field is part of a repeat group that includes the KEY, VOLSER, PROFTYPE, and SENSTYPE fields. The default and maximum length is 35 characters. An example value is IPO1.CICS.CICSTS41.DATASET. The format is as follows:

system.subsys-type.subsys-identification.restype

STAMP

Returns the unload time stamp of the RACF database. It cannot be used for `SELECT` and `EXCLUDE` processing.

VIA

Shows either a keyword in dashes or a user ID or group name that was instrumental in getting the access to the resource. For example, the value can be a connect group of the ID. If access was permitted through class authorization, the field value contains the user ID. To provide users with the ability to modify (overtype) this value, use the ACCESS_VIA_WHEN field instead of VIA.

Table 416. REPORT_SCOPE VIA field keywords and descriptions

Keyword	Description
-AUDIT-	Audit access permitted by the group=auditor attribute.
-CREATE-	Access permitted by connect authority of CREATE, JOIN or CONNECT. This access is even honored for revoked connects.
-CLAUTH-	Access permitted by user ID class authorization. Class authorization applies by POSIT number, and SETROPTS GENERICOWNER does not restrict adding profiles and members in a grouping class.
-GLOBAL-	Access permitted by the global access table.
-OPER-	Access permitted by the group-operations attribute.
-RACDCT-	Access permitted through an IRR.DIGTCERT.*function* resource in the FACILITY class.
-RACMAP-	Access permitted by the IRR.RACMAP.*function* resource in the FACILITY class.
-SCP.G-	Resource in scope due to access permitted on a CKG.SCP.G... scope check.
-SCP.ID-	Resource in scope due to access permitted on a CKG.SCP.ID... scope check.
-SCP.U-	Resource in scope due to access permitted on a CKG.SCP.U... scope check.
-UACC-	Access permitted through universal access.
-UNPROT-	Resource is not protected.
-WARN-	All access permitted due to warning mode.

VOLSER

Repeat group field that includes the KEY value. On the first or only line of an entry, this group field shows the volume serial for the RACF profile in the KEY field. This information is provided only for discrete profiles. In the subsequent lines, the volume serial is shown for the volume where the data sets in the corresponding line of the KEY are stored. The data set volume serial numbers are present only when the REPORT DATASETS option has been specified.

WHEN

Provides the class and profile name that must be in control for access to be permitted by RACF. To provide users with the ability to modify (overtype) this value, use the ACCESS_VIA_WHEN field instead of the VIA field.

REPORT_SENSITIVE: Sensitive data sets by profile

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

The REPORT_SENSITIVE NEWLIST (NEWLIST TYPE=REPORT_SENSITIVE) has been designed to verify that sensitive data sets are adequately protected. Updates must be tightly controlled for some data sets like APF data sets, security databases, and page or swap data sets. For other data sets like the security database and page or swap data sets, read access to the information must be tightly controlled. zSecure Collect recognizes some sensitive data sets automatically. zSecure Admin and zSecure Audit verify RACF protection according to either *confidentiality* or *integrity* demands. The sensitive data sets checked automatically are:

- APF data sets (integrity)
- LPA data sets (integrity)
- Linklist data sets (integrity)
- Page data sets (confidentiality and integrity)
- System Storage Index data sets (confidentiality and integrity)
- Swap data sets (confidentiality and integrity)
- RACF data sets (confidentiality and integrity)
- SMF recording data sets (confidentiality and integrity)
- System dump data set (confidentiality and integrity)
- TSO user administration data set UADS (confidentiality and integrity)
- Other system data sets: SYS1.NUCLEUS and SYS1.LPALIB (integrity)
- JES2 and JES3 checkpoint data sets (confidentiality and integrity)
- JES2 and JES3 spool data sets (confidentiality and integrity)
- JES2 and JES3 parameter data set (confidentiality and integrity)
- JES2 and JES3 STC/TSU/JOB proclib (integrity, but only when SIMULATE SENSITIVE PROCLIB has been specified)
- JES2 spool offload data set (confidentiality and integrity)
- MSTR proclib (integrity)
- MSTR parameter library (integrity)
- MSTR VIO administration (integrity)
- DFHSM data set BCDS, MCDS, OCDS (integrity)
- DMS database DMSFILES (integrity)
- DMS authorized parameter library (integrity)
- DMS default parameter library (integrity)
- CA1 tape management catalog TMC (integrity)
- DFSMS SCDS and ACDS (integrity)
- IODF file, if DSN could be found (integrity)
- RMM control dataset and parmlib (integrity)
- TLMS volume master file VMF (integrity)
- ABR archive control file ACF (integrity)
- IPL load parameter data sets (integrity)
- HFS and zFS data sets (integrity)
- RRSF IN/OUT data sets (confidentiality and integrity)
- IEFJOBS data sets (integrity)
- Catalog data sets (ALTER)
- CS Resolver configuration files (integrity)

You can add your own data sets using the SIMULATE SENSITIVE command. See "SIMULATE" on page 911. LINKLIST data sets are automatically reported as APF

data sets, unless the IEASYSxx member in your system contains LNKAUTH=APFLST. If LINKLIST data sets are not automatically APF authorized, you can use the SIMULATE SENSITIVE LINKLIST command to report LINKLIST anyhow. SIMULATE SENSITIVE PROCLIB can be used to flag integrity problems in the JES2 proclibs used for batchjobs.

The security policy adhered to conforms to the DOD 5200.28-STD standard ('Orange Book') at C2 level or to the Common Criteria V1.0 profile CS1.

The security policy adhered to for *confidential* data sets is:

1. Confidential data sets must be protected against READ access.
2. READ access must be audited.
3. Information must be erased physically when deleted.

The security policy adhered to for *integrity-sensitive* data sets is:

1. Integrity-sensitive data sets must be protected against UPDATE.
2. UPDATE access must be audited.

For the check on audit trail on RACF systems, both AUDIT and GLOBALAUDIT settingsare checked. GLOBALAUDIT is not checked in PADS mode if you don't have the AUDITOR attribute. In addition, the LOGOPTIONS setting is considered as well as SECLEVELAUDIT and SECLABELAUDIT settings when SECLEVELs or SECLABELs are active. The check is passed if any of these settings provides the required level of auditing.

The REPORT_SENSITIVE NEWLIST returns a record for each sensitive data set found, grouped by the covering data set profile.

The CARLa script CKRRSENS containing this NEWLIST type is included automatically by the REPORT SENSITIVE command if the NEWLIST type was not yet specified in the command input preceding the REPORT command.

Field descriptions

The REPORT_SENSITIVE NEWLIST provides the following fields for reporting.

ACCESS

This repeat group field returns the access level column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

AUDITCONCERN,CONCERN

This field returns a concatenation of audit concerns for the profile. Table 417 shows the default audit priority and concerns. The priority can be higher due to a SIMULATE POLICY statement.

Table 417. REPORT_SENSITIVE: AUDITCONCERN priorities and descriptions

Priority	Audit Concern	Description
60	Unprotected	There is no profile protecting the data set, and PROTECTALL(FAILURES) is not set
55	Global access	The access given through the Global Access Table is too high
50	UACC too high	Universal access should be NONE or READ
45	ID(*) too high	ID(*) on the access list has too high access
45	Warning mode access	Warning mode on profile resulted in ALTER access

Table 417. REPORT_SENSITIVE: AUDITCONCERN priorities and descriptions (continued)

Priority	Audit Concern	Description
35	No erase	Erase on scratch required for confidentiality
15	Read fail audit	Read failure audit required for confidentiality
15	Update fail audit	Update failure audit required for integrity
15	Alter fail audit	Alter failure audit required for integrity
10	No read audit	Read audit required for confidentiality
10	No update audit	Update audit required for integrity
10	No alter audit	Alter audit required for integrity

The command VERIFY SENSITIVE can be used to generate RACF commands that remedy profile deficiencies.

AUDITF

This returns the lowest access level that results in auditing of access attempt failures. It is empty if failure auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

AUDITLVL

This field is a combination of the fields AUDITS and AUDITF ; contrary to these, it supports overtype . This field is not available for selection. Use AUDITS and AUDITF instead.

This field returns the audit priority for the profile. See field AUDITCONCERN for a table with the concerns and their priorities. The actual audit priority can be higher because of e.g. a SIMULATE POLICY C2 statement.

AUDITS

This returns the lowest access level that results in success auditing. It is empty if success auditing is inactive.

The reported value for the access level is derived from the following settings:

- Profile settings (including the GLOBALAUDIT settings when you are an auditor).
- LOGOPTIONS settings for the class
- Any SECLEVEL or SECLABEL settings, if SECLEVEL or SECLABEL auditing is active.

This field does not support overtype, use AUDITLVL instead.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

ERASE

This flag field shows whether erase-on-scratch is active for the profile. It only shows the profile flag. To be used, the corresponding SETROPTS and HSM settings must also be on. This field supports overtype.

ID

This repeat group field returns the user or group ID column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

KEY

For RACF, this repeat group field returns the profile name covering the sensitive data sets on the first line. On subsequent lines, the (sensitive) data sets it covers are listed. It is part of the same repeat group as PROFTYPE, SENSTYPE and VOLSER. If the REPORT DATASETS option has been added (specify behind your NEWLIST requests), then all non-sensitive data sets covered will be included as well.

MARK

This repeat group field returns the annotation column of the combined access list defined by MARK, ID, ACCESS, and PROGRAM The field contains an arrow '->' to highlight a specific access list entry that has a problem.

ORDER

This field returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

OWNER

This field returns the owner of the RACF profile. This field supports overtype.

PAGEBY

This field returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PROFTYPE

This repeat group field returns RACF profile the type of (missing, GENERIC, NONVSAM, TAPE or MODEL) on the first line, and the type of data set for a data set repeat group entry (nvsam, clust, tape, etc.) on subsequent lines. It is part of the same repeat group as KEY, PROFTYPE, SENSTYPE and VOLSER. Table 418 shows the data set types and their meaning.

Table 418. REPORT_SENSITIVE: PROFTYPE dataset types and descriptions

bkpclu	Backup of a VSAM cluster. Normally, this is only listed below a backed-up discrete profile (for example, a discrete profile with a system-generated name). The source for the cluster name is the HSM BCDS or a DMS DMSFILES data set.
clustr	VSAM cluster (catalog entry). The volume listed is the volume of the catalog. The source for the cluster names can be a catalog, HSM MCDS, ABR ACF, DMS DMSFILES data set, or VVDS.

	index	Index component of a VSAM cluster residing on the indicated DASD volume.
	data	Data component of a VSAM cluster residing on the indicated DASD volume.
	aixix	Index component of a VSAM alternate index residing on the indicated DASD volume.
	aixda	Data component of a VSAM alternate index residing on the indicated DASD volume.
	migcl	Migrated or archived VSAM cluster. This is listed below a cluster entry instead of the components. The volume is equal to MIGRAT or ARCIVE.
	clust	Backup of VSAM cluster. This is listed below a bkpclu entry instead of the components. The volume is equal to MIGRAT or ARCIVE.

cmmtap	Cataloged, managed tape file on a managed, non-scratch tape volume.
cnmtap	Cataloged, non-managed file on a managed, non-scratch volume. This means that the catalog entry conflicts with the tape management information.
cnntap	Cataloged, non-managed tape file, on a non-managed volume.
cnstap	Cataloged, non-managed file, on a managed volume in scratch status.
gdg	Base name of a GDG (Generation Data Group), obtained from a catalog.
mdisk	VM minidisk. The minidisk resource name has the form USERID.DEVN or ACIGRP.USER.DEVN
notfnd	Data set name is in some table but the data set itself does not exist.
nvsam	Non-VSAM disk data set, migrated if volume is MIGRAT (for HSM or ABR) or archived if the volume is ARCIVE (for DMS). This information is obtained from the VTOC for data sets on disk, the HSM MCDS and the ABR ACF for migrated data sets, and the DMSFILES data set for archived data sets. The information is not derived from the catalog entries.
priv	General resource name where even access less than READ is a sensitive privilege.
secvol	Secondary volume of a multi-volume data set.
sens-a	General resource name where ALTER access is sensitive.
sens-r	General resource name where READ access is sensitive.
sens-w	General resource name where WRITE access is sensitive.
ummtap	Uncataloged, managed tape file on a managed, non-scratch tape volume.
unmtap	Uncataloged, non-managed file on a managed, non-scratch volume. The source for such an entry is probably the TVTOC of a TAPEVOL profile.
unntap	Uncataloged, non-managed tape file, on a non-managed volume. The source for such an entry is probably the TVTOC of a TAPEVOL profile.
unstap	Uncataloged, non-managed file, on a managed volume in scratch status. The source for such an entry is probably the TVTOC of a TAPEVOL profile.

PROGRAM

This repeat group field returns the program conditional access column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

RESOURCE_LOCATION

Identifies the resource name environment. This field is part of a repeat group that includes the KEY, VOLSER, PROFTYPE, and SENSTYPE fields. The default and maximum length is 35 characters. An example value is IPO1.CICS.CICSTS41.DATASET. The format is as follows:

system.subsys-type.subsys-identification.restype

PROGRAM

This repeat group field returns the program conditional access column of the annotated combined access list defined by MARK, ID, ACCESS, and PROGRAM.

SENSTYPE

This repeat group field denotes the type of sensitivity of an individual data set. It is part of the same repeat group as KEY, PROFTYPE, SENSTYPE, and VOLSER.

In case of multiple sensitivities for a single data set, only the prime sensitivity or sensitivities are represented. For instance, a data set can be a MSTR parmlib, a JES2 parmlib, an STC proclib and a JOB proclib all at the same time. In this case, JES2 parmlib will win because that data set might contain human readable passwords.

STAMP

This field returns the time stamp of the security database. It cannot be used for SELECT/EXCLUDE processing.

UACC

For a RACF system, this field returns the combined universal access of the profile UACC, the global access table, and the protectall setting (in case the profile is missing). This field supports overtype.

VOLSER

This field is a repeat group with KEY PROFTYPE, SENSTYPE, and VOLSER. On the first line it shows the volume serial of the RACF profile in the KEY field (only filled in if it is a discrete). On the following lines the volume serial where the data sets in the corresponding line of KEY reside is shown.

REPORT_STC: Started procedure protection

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	

The `REPORT_STC NEWLIST` (`NEWLIST TYPE=REPORT_STC`) helps determine which started procedures pose a risk to the installation. This `NEWLIST` returns a record for each JCL member that can be started with the `START` command.

The CARLa script CKRRSTC containing this `NEWLIST` type is included automatically by the `REPORT STC` command if the NEWLIST type was not yet specified in the input above the `REPORT` command.

The consistency of the three information sources (ICHRIN03, RACF database, and procedure libraries) can be verified by running the VERIFY STC command.

Field descriptions

The REPORT_STC NEWLIST provides the following fields for reporting.

AUDITOR

Flag field that indicates in a RACF system that the started procedure will run with a RACF userid that has system-wide AUDITOR authority.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

CONCAT

This field is part of a repeat group together with the field SUBSYS It lists the sequence number of the procedure library listed by DSN in the concatenation. Each subsystem on each system can have its own concatenation. See also HIDDEN

DSN

The field lists the data set name of the started procedure library where the JCL member resides.

FLAGS

This is a text field that contains special authorizations or conditions for the started task. This information comes from the RACF user profile and connect definition, from the Start Procedure Table ICHRIN03 entry, or from the RACF STARTED profile. A letter can be displayed at a specific column. Table 419 describes the possible values for this field..

Table 419. REPORT_STC Flags field - Available values

Flag	Description
*	An unusual condition exists for this task, a database or table mismatch for example. The reason might be found by running VERIFY STC.
r	The user assigned to the started procedure is revoked. Depending on your RACF and PTF level, the task cannot be started because it is revoked, or the task will run with reduced functionality. It might have problems submitting batch jobs, allocating new SMS-managed data sets, or obtaining printed output.
s	System-wide SPECIAL authority.
o	System-wide OPERATIONS authority.

Table 419. REPORT_STC Flags field - Available values (continued)

Flag	Description
a	System-wide AUDITOR authority.
p	The task is privileged. This means that all access requests (except those that request a profile to be returned in-storage through the use of the CSA or PRIVATE keywords) are granted and auditing is suppressed.
t	The task is trusted. This means that all access requests (except those that request a profile to be returned in-storage through the use of the CSA or PRIVATE keywords) are granted and only limited auditing possibilities exist. Auditing is only possible via SETROPTS LOGOPTIONS and the UAUDIT setting for the userid.
D	The group specified in the Started Procedures Table or the STARTED profile is the default group for the user. [12]
S	The procedure uses a RACF STARTED profile.
3	The procedure uses ICHRIN03.

GROUP

The current connect group that is used if the task is started.

GROUP_DFLTGRP

For a RACF system, this flag field indicates that the started task runs under the default group for the RACF user.

HIDDEN

Flag field that indicates that the procedure JCL is hidden from view in the STC proclib concatenation. This can happen if there is a similarly named member in a procedure library concatenated in front of this library.

ICHRIN03

Flag field that indicates in a RACF system that the procedure name is part of the started task table ICHRIN03.

ISPF_DATE

The last modification date in the ISPF statistics of the JCL member. This has only documentary value and no security relevance since it can be changed at will by the updater. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see “Date fields” on page 903.

ISPF_USERID

This is the userid present in the ISPF statistics of the JCL member. This has only documentary value and no security relevance since it can be changed at will by the updater.

LAST_CHANGE

This field indicates the date and time when the JCL member was last changed or when it was created, whichever is more recent. If the current JCL member version belongs to a PDSE data set and has extended member statistics, this

12. Job submission from started tasks used to be protected by assuring that the started task RACF user default group was a RACF group specifically for started tasks, and making sure that the connect to this group was revoked. This construction made sure that no job could be submitted without a password. Since the class PROPCNTL has been introduced this mechanism can be replaced by a profile for the started task in that class. In addition, it is now customary to allow submission with a GROUP= parameter on the JOB card without specifying a password, so the old protection mechanism does not really work anymore.

field provides the extended member statistics. Otherwise, this field provides ISPF statistics information for the member which includes the ISPF_DATE. For information on using this field in SELECT and EXCLUDE statements, see "Combined date and time fields" on page 904.

LAST_CHANGE_USERID

This field indicates the user ID that was last used to modify the JCL member. If the current JCL member version belongs to a PDSE data set and has extended member statistics, this field provides the user ID taken from the extended member statistics. Otherwise, this field provides the user ID taken from the ISPF statistics for the member. (See "ISPF_USERID" on page 1248.)

OPERATIONS

Flag field that indicates in a RACF system that the started procedure will run with a RACF userid that has system-wide OPERATIONS authority.

ORDER

This field returns a number that when sorted corresponds to the sort order designated by the REPORT BY= parameter. It can be used with the modifier NONDISPL to implement the REPORT BY= parameter.

PAGEBY

This field returns a number that increases at each page break implied by the REPORT PAGEBY= parameter. It can be used with the modifiers PAGE,NONDISPL to implement the REPORT PAGEBY= parameter.

PRIVILEGED

Flag field that indicates in a RACF system that the started procedure runs with the privileged attribute. All access requests (except those that request a profile to be returned in-storage through the use of the `CSA` or `PRIVATE` keywords) are granted and auditing is suppressed. If the `PRIVILEGED` flag is set, RACF ignores the value of the `TRUSTED` setting. Accordingly, the `REPORT_STC NEWLIST` reports the `TRUSTED` flag as not set.

PROCNAME

The name of the procedure JCL member in the procedure library. This name is used on the START command to start the task.

PROFILE

The RACF STARTED profile, if one is found.

PROTECTED

This flag field indicates whether the user ID associated with the started task is protected or not. A protected user ID does not have a password and cannot be revoked by entering incorrect passwords.

SPECIAL

Flag field that indicates in a RACF system that the started procedure will run with a RACF userid that has system-wide SPECIAL authority.

STAMP

This field returns the unload time stamp of the security database. It cannot be used for SELECT/EXCLUDE processing.

SUBSYS

This field is the key of a repeat group with the field CONCAT. It lists the subsystem name the output line applies to. The START command can be issued with this subsystem name in the SUB= parameter. The SUB= parameter is required to direct the START command to a subsystem other than the default (primary) subsystem.

SYSTEM

This is the SMF id of the system NEWLIST record applies to. Note that each system can have its own Started Procedure Table ICHRIN03, even while sharing the RACF database.

TRUSTED

For a RACF system, this flag field indicates that the started procedure runs with the trusted attribute. All access requests (except those that request a profile to be returned in-storage through the use of the CSA or PRIVATE keywords) are granted and only limited auditing possibilities exist. Auditing is only possible via SETROPTS LOGOPTIONS and the UAUDIT setting for the userid. If the PRIVILEGED flag is set, RACF ignores the value of the TRUSTED setting. Accordingly, the REPORT_STC NEWLIST reports the TRUSTED flag as not set.

UACC

This field returns the universal access of the JCL member. If this is UPDATE, and the started task has system level authorities, then a major leak exists. If it is UPDATE and the userid has no system level authorities, a trojan horse risk exists. If it is READ then this is of value to hackers if they have found a way to issue a START command. This field is only present for RACF systems.

USERID

This field lists the userid assigned by the RACF Started Procedure Table ICHRIN03, or by a STARTED profile. This field can contain *, this is the default RACF user for a task originating from within the system. If you want to suppress these report lines, specify SUPPRESS ID=*. For an invalid STARTED profile, this column can contain ++++++++, which is the 'undefined' user.

VOLSER

This field lists the volume serial where the procedure library listed by field DSN resides.

ROUTER: SAF Router Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The ROUTER NEWLIST (NEWLIST TYPE=ROUTER) displays the SAF (System Authorization Facility) router table. It generates one entry per entry in the table. A unique key is SYSTEM ORDER.. Unless otherwise noted, you can use all fields for SELECT and EXCLUDE processing as well as in the following output commands: LIST, SORTLIST, SUMMARY, and DISPLAY.

Field descriptions

The ROUTER NEWLIST provides the following fields for reporting.

ACTION

This string indicates the action to be taken for this requestor, class, and subsystem. It has the value 'NONE' when RACROUTE requests are to be ignored (RC=0), and 'RACF' when RACF is to be called, for example, a value of 'NONE' indicates that authorization requests by the indicated requestor and subsystem for the indicated class is allowed without checking any profiles.

AUDITCONCERN, CONCERN

This field indicates the reason for the audit priority. You should not use the exact value of this field as a programming interface. The audit concern currently defined is:

- Class not in CDT

  This means that SAF (System Authorization Facility) cannot pass a security check in this class to RACF, because RACF does not know it. If the router table indicates it is passed to RACF, this is given priority 15; if not, 3.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 420. ROUTER NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CLASS, C

The class name passed to the RACROUTE call.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

INCDT

This flag indicates whether the current class is included in the Class Descriptor Table (CDT, see NEWLIST TYPE=CLASS). Normally, the only non-general resource classes that can have INCDT=NO are DATASET, USER, CONNECT, and GROUP.

ORDER, ORG

The original order (entry number) of this class entry in the RACF router table. The first entry in the table has ORDER=1.

REQSTOR

The requestor name passed to the RACROUTE call.

SUBSYS

The subsystem name passed to the RACROUTE call.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters to cater to VM systems.

RRNG: RACF Database Range Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The RRNG NEWLIST (NEWLIST TYPE=RRNG) describes the RACF Database Range Table. This table determines which RACF profiles are stored in which RACF data set. This NEWLIST generates one entry per key range per system. A unique key is SYSTEM ORDER. It displays the in-storage range table loaded from module ICHRRNG during IPL. Unless otherwise noted, you can use all RRNG NEWLIST fields for SELECT and EXCLUDE processing as well as in the following output commands: LIST, SORTLIST, SUMMARY, and DISPLAY.

Field descriptions

The RRNG NEWLIST provides the following fields for reporting.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

DB

RACF data set sequence number. This number identifies the data set in the Database Name Table (DSNT) that must be used for this key range. Information on these data sets can be displayed with a NEWLIST TYPE=DSNT.

KEY

Lowest profile key for this data set. Profiles with keys higher than or equal to this key (and lower than the next lowest key in the table) are routed to the data set with a sequence number DB (value of the DB parameter). Unreadable characters are *not* replaced by a period.

KEYHEX

Lowest profile key for this database, in hexadecimal format. Profiles with keys higher than or equal to this key (and lower than the next lowest key in the table) are routed to the data set with sequence number DB.

ORDER, ORG

The original order (entry number) of this entry in the resource range table. The first entry in the table has ORDER=1.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters to cater to VM systems.

RRSFNODE: RRSF configuration information

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•			•	•	•

The RRSFNODE NEWLIST (NEWLIST TYPE=RRSFNODE) returns the RRSF node information for the current system configuration. The information is obtained from existing CKFREEZE files. This NEWLIST type supports processing multiple CKFREEZE files to provide a multinode view of the entire configuration.

Note: For information about NEWLIST statements, processing, and formatting options, see "NEWLIST" on page 846.

Field descriptions

The RRSFNODE NEWLIST provides the following fields for reporting.

ADDRESS
The host name or IP address entered on the TARGET command when defining an RRSF node with TCP protocol.

APPC_LUNAME
Logical Unit name for RRSF connection to the TARGET_NODE if the APPC communication protocol is APPC.

APPC_MODENAME
SNA mode name designating the network properties to be used when setting the APPC connection to the TARGET_NODE.

APPC_TPNAME
The APPC Transaction Profile Name (TPNAME). The value returned can have between one and 64 characters.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX
Name of the security complex that contains the system where the RRSF node is defined. The value returned can be from the ALLOC COMPLEX parameter or default to a system name.

DESCRIPTION
The user-specified description for this RRSF node.

IS_LOCAL
Flag field (Yes/No) that indicates whether this node is designated as the local node for SYSTEM.

IS_MAIN
This Flag field (Yes/No) that indicates if this system is the main system in the RRSF node.

LOCAL_NODE
The name of the local RRSF node for this system.

PORTNUM
The port number entered on the TARGET command when defining an RRSF node with TCP protocol.

PROTOCOL
Protocol for communication. The value can be APPC (Advanced Program-to-Program Communications) or TCPIP for (Transmission Control Protocol/Internet Protocol).

SYSTEM
Name of the system where the RRSF node is defined.

TARGET_NODE
The name of the remote RRSF node.

TARGET_SYSNAME
The (GRS) name of the remote system. The target node is local to this system.

TARGET_SYSTEM
The (SMF) name of the remote system. The target node is local to this system.

TARGET_COMPLEX
The target system is a member of this complex.

TARGET_STATE
The state of the remote RRSF node. Table 421 lists the possible state values.

Table 421. RRSF node state values

Value	Description
O_A	Operative Active
O_P_C	Operative Pending Connect
O_P_V	Operative Pending Verify
O_E	Operative Error
D_L	Dormant Local
D_R	Dormant Remote
D_B	Dormant Both
D_E	Dormant Error
???	Unknown state

USERID
The ID of the user that created this RRSF node definition.

WORKSPACE_PREFIX
The high-level qualifiers for the workspace data set. This value is specified by the PREFIX keyword on the TARGET command. The format for the prefix value is different for local and remote data sets. For a local workspace data set, the prefix is specified as `prefix .sysname | wdsqual .INMSG | OUTMSG`. For data sets available through a remote connection, the prefix is formatted as `prefix . local_luname . remote_luname | wdsqual . INMSG | OUTMSG`.

WORKSPACE_QUALIFIER
The middle qualifier for the workspace data set name. This value is specified by the WDSQUAL keyword on the TARGET command.

WORKSPACE_VOLUME
The volume serial number for the workspace data set if configured.

WORKSPACE_FILESIZE
The file size for the DEFINE CLUSTER of a VSAM workspace data set. This value represents the maximum number of entries that the data set can hold.

WORKSPACE_DATACLAS
The SMS DATACLAS for the workspace data set.

WORKSPACE_STORCLAS
The SMS STORCLAS for the workspace data set.

WORKSPACE_MGMTCLAS
The SMS MGMTCLAS for the workspace data set.

SENSDSN: Sensitive Data Set Names

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•			•	•	•

The SENSDSN NEWLIST (NEWLIST TYPE=SENSDSN) describes the sensitive data set names, taken from the in storage APFLIST, LINKLIST, and LPALIST tables, and from common and private system and subsystem control blocks. Each entry in this NEWLIST represents one sensitive data set, and is uniquely identified by the fields SYSTEM DATASET VOLSER.

A SENSDSN NEWLIST (NEWLIST TYPE=SENSDSN) comparison report can show a change for a sensitive data set that is accessible from only one of the systems being compared. This occurs because a sensitive data set from any of the input CKFREEZE files is considered as sensitive on the other systems as well. However, when a sensitive data set resides on a non-shared DASD, it is treated as not mounted on some systems and mounted on other systems. A CKFREEZE file for each system does not provide any information about the DSN and volume inventory on any other system. When multiple CKFREEZE files are input to the comparison, the volsers and data sets are treated as if they were potentially sensitive in every system. This design provides a report that shows a consolidated overview of all the sensitive data sets and their status in the entire combined environment. Consequently, a sensitive data set is considered sensitive everywhere, even if the data set was not accessible from a system when the CKFREEZE file was created.

Field descriptions

The SENSDSN NEWLIST provides the following fields for reporting.

APF

This flag field indicates whether the data set is APF-authorized. The data set is part of the APFlist, the linklist if it is authorized, or the LPAlist.

Note: A data set can be part of the APFlist and not be APF-authorized. In that case, the APF flag is not set, and the APFLIST flag is set. The following reasons for this exist:

- The data set named in the APF list does not have a volume serial, but is cataloged to a non-SMS-managed volume.
- The data set named in the APF list is an alias.
- The data set named in the APF list has a volume serial, but no such data set exists.

- The data set named in the APF list has a volume serial, but the volume is not mounted.
- The data set named in the APF list does not have a volume serial, but is not cataloged.

In this, Security zSecure follows the MVS rules.

APFLIST

This flag field indicates whether the data set is part of the APFlist, or part of the linklist if it is authorized.

AUDITCONCERN, CONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The AUDITCONCERN field can contain one or more concerns separated by commas. The following audit concerns have currently been defined:

In APFlist but no volser and not cataloged to SMS-managed volume

The data set is in the APFlist without volume serial, but the data set is cataloged to a non-SMS-managed volume. The data set is not APF-authorized.

In APFlist but an alias

The data set is in the APFlist but is an alias. The data set is not APF-authorized.

In APFlist but data set not on volume
The data set is in the APFlist with volume serial, however no such data set exists.

In APFlist but volume not mounted

The data set is in the APFlist with volume serial, but the volume is not mounted. The data set is not APF-authorized.

In APFlist but data set not cataloged

The data set is in the APFlist without volume serial but the data set is not cataloged. The data set is not APF-authorized.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 422. SENSDSN NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

BOX_SERIAL

This field describes the DASD unit's volume serial number and device id for the data set. This field can be used to disambiguate between DASD volumes with the same VOLSER. See also “BOX_SERIAL field for DASDVOL report” on page 1014.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

DATASET, DSN

This field contains the data set name. When combined with the SYSTEM and VOLUME fields, this field uniquely identifies an entry in the NEWLIST TYPE=SENSDSN.

ERASE

This field is empty in Security zSecure.

LINKLIST

This field indicates the linklist concatenation number of the data set, if it is part of the linklist.

LNKAUTH

This flag field indicates whether the data set is in the linklist and the linklist is considered APF-authorized (because of a LNKAUTH=LNKLIST in the effective IEASYSxx parmlib member).

LPALIST

This flag field indicates the LPAlist concatenation number of the data set, if it is part of the LPAlist.

MOUNTED

This flag field indicates whether the data set volume is mounted. In this release, this flag is only valid if the DASDVOL report is also used.

RESOURCE_LOCATION

Identifies the resource name environment. This field is repeat group field. The default and maximum length is 35 characters. An example value is IPO1.CICS.CICSTS41.DATASET. The format is as follows:

system.subsys-type.subsys-identification.restype

RISK

This field indicates the lowest access level considered an exposure, which is dependent on the data set sensitivity type. Possible RISK values are READ, UPDATE, and ALTER.

Data set types with a READ risk

ACF2 databases, alternate clusters and backup databases

ICSF key data sets CKDS, PKDS, and TKDS

JES2 parameter, checkpoint, spool and spool offload data sets

RRSF IN/OUT data sets
SMF recording data sets
System dump, page, and swap data sets
UADS data set

Data set types with an UPDATE risk

Aliases in the APFlist
ABR archive control file (ACF)
ACF2/CICS parameter library (CICS ACF2pr)
ACF2 MAINT, BLPPGM and LINKLST record libraries
APF list data sets
CA1 tape management catalog (TMC)
CICS program library (CICS Loadlb).
CICS resource definition data set (CICS CSD)
CICS parameter library (CICS Parms)
Communications Server configuration and include files
Couple data sets (Primary and Alternate)
CS Resolver configuration files
DB2 Bootstrap data set (BSDS)
DMS database and parameter libraries
HSM MCDS, OCDS, and BCDS data sets
HFS and zFS data sets
IMS program library (IMS PROCLIB)
IPL nucleus data set
IPL parameter libraries
JES2 and JES3 STC/TSU/JOB proclibs
LPA list data sets
Linklist data sets
RMM parameter library and control data sets
SMS ACDS, COMMDS, and SCDS data sets
Storage index data set
System active IODF data set
System IEFJOBS data sets
System parameter library
System REXX library
TLMS volume master file (VMF)
UNIX zFS file system in a VSAM linear data set (zFS data set)

Data set types with an ALTER risk

Catalogs
Data sets in the APF list with a volume serial that does not exist
Data sets in the APF list with a volume serial that is not mounted
Data sets in the APF list without a volume serial that are cataloged to a non-SMS-managed volume
Data sets in the APF list without a volume serial that are not cataloged

SENSITIVITY

This field indicates the type of sensitivity of the data set. The following sensitivity types have been defined:

Table 423. SENSDSN: Sensitivity types and descriptions

Sensitivity	Meaning
ABR ACF	ABR Archive Control File (ACF)
Active IODF	System active IODF data set
APF library	APF library, not in linklist or LPAlist
APF lib+Lnk	Library in APFlist and linklist, not in LPAlist
APF linklst	Library in linklist (authorized), not in APF list, nor in LPA list
APF LPA+Lnk	Library in APF list, LPA list and linklist
APF LPAlist	Library in APF list and LPA list, not in linklist
CA1 TMC	CA1 Tape Management Catalog (TMC)
Catalog	Catalog data sets
CICS Loadlb	CICS program library
CICS CSD	CICS resource definition data set
CICS Parms	CICS parameter library
CICS ACF2pr	ACF2/CICS parameter library
Couple Alt	Alternate couple data set
Couple Prim	Primary couple data set
CSconfig	Default library found in the standard Communications Server configuration file search sequence
CSinclude	Communications Server include file
DB2 BootSDS	DB2 Bootstrap data set (BSDS)
DftTCPIPDta	CS Resolver default TCPIP.DATA file
DftIPNODES	CS Resolver default IPNODES file
DMS AuthPrm	DMS authorized parameter library
DMS parmlib	DMS default parameter library
DmsFiles	DMS DMSFILES database
HFS data set	HFS
GlbTCPIPDta	CS Resolver default TCPIP.DATA file
GlbIPNODES	CS Resolver global IPNODES file
HSM BCDS	HSM BCDS data set
HSM MCDS	HSM MCDS data set
HSM OCDS	HSM OCDS data set
ICSF CKDS	Cryptographic Key data set with encrypted symmetric keys
ICSF PKDS	Cryptographic Key data set with encrypted asymmetric (public/private) key
ICSF TKDS	Data set with cryptographic tokens (encrypted or clear)
IMS PROCLIB	IMS program library.
IPL LoadPrm	Library in logical parmlib concatenation used at IPL
IPL nucleus	z/OS nucleus data set, executable code loaded at IPL time
JES2 Ckpt	JES2 checkpoint data set

Table 423. SENSDSN: Sensitivity types and descriptions (continued)

Sensitivity	Meaning
JES2 prmlib	JES2 parameter library
JES2 Spool	JES2 spool data set
JES3 Ckpt	JES3 checkpoint data set
JES3 prmlib	JES3 parameter library
JES3 Spool	JES3 spool data set
JOB proclib	JES2 or JES3 JOB proclib (this sensitivity type is only shown when SIMULATE SENSITIVE PROCLIB has been specified)
Linklist	Linklist library (not authorized), not in APF list, nor in LPA list
LPA+APF Lnk	Library in LPAlist and linklist (authorized), not in APF list.
LPA+Linklst	Library in LPA list and linklist (not authorized), not in APF list
LPAlist	LPA list library, not in APF list, nor in linklist
MSTR prmlib	Master parameter library
MSTR STClib	Master Started Procedure library
NoAPF alias	Alias in the APFlist
NoAPFnonSMS	Library in the APFlist without a volser, but cataloged to a non-SMS-managed volume
NoAPFnoCtlg	Library in the APF list without a volume serial, but not cataloged
NoAPFnotMnt	Library in the APF list with a volume serial, but the volume is not mounted
NoAPFnoDsn	Library in the APF list with a volume serial, but the data set does not exist
Offload	JES2 spool offload data set
Pagedataset	System page data set
RACF back	RACF backup database
RACF prim	RACF primary database
ResolvSetup	CS Resolver setup file
RMM Control	RMM control data set
RMM parmlib	RMM parameter library
RRSFdataset	RRSF IN/OUT data set
Sens Read	READ sensitive on another system, but also available on this system
Sens Update	UPDATE sensitive on another system, but also available on this system
SMF dataset	SMF recording data set
SMS ACDS	SMS ACDS data set
SMS COMMDS	SMS COMMDS data set
SMS SCDS	SMS SCDS data set
STC joblib	System IEFJOBS data set
STC proclib	JES2 or JES3 STC proclib
StgIndex	System Storage Index data set
Swapdataset	System swap data set
System Dump	System dump data set

Table 423. SENSDSN: Sensitivity types and descriptions (continued)

Sensitivity	Meaning
System REXX	Library with REXX programs that execute APF authorized
TLMS VMF	TLMS Volume Master File (VMF)
TSO UADS	UADS data set
TSU proclib	JES2 or JES3 TSU proclib
zFS data set	UNIX zFS file system (in a VSAM linear data set)

In case there are multiple sensitivities for a single data set, only the prime sensitivity or sensitivities are represented. For instance, a data set can be a MSTR parmlib, a JES2 parmlib, an STC proclib and a JOB proclib all at the same time. In this case it will be shown as a JES2 parmlib, because that data set can contain human readable passwords.

Note that for data sets on the LPA list and linklist the APF flag might be set. This is because the LPA, where a program is first searched for when no JOBLIB/STEPLIB is specified, is always treated as APF-authorized. The linklist, where the program is searched next, when it was not found in LPA, is likewise treated as APF-authorized if the effective IEASYSxx member in your parmlib specifies LNKAUTH=LNKLST.

SYSPLEX

The name of the sysplex the SYSTEM is a part of (if applicable).

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types. When combined with the DATASET and VOLUME fields, this field uniquely identifies an entry in the NEWLIST TYPE=SENSDSN.

VOLSER, VOLUME

For non-VSAM data sets this field contains the volume serial of the data set. For VSAM data sets it is missing. When combined with the SYSTEM and DATASET fields, this field uniquely identifies an entry in the NEWLIST TYPE=SENSDSN.

VOLSER_OR_SMS

For non-VSAM data sets, this field contains the volume serial of the data set unless the volume is SMS-managed, in which case the field contains *SMS*. For VSAM data sets, the field is missing. When combined with the SYSTEM and DATASET fields, this field uniquely identifies an entry in the NEWLIST TYPE=SENSDSN.

SETROPTS: System-wide RACF Options in database

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The SETROPTS NEWLIST (NEWLIST TYPE=SETROPTS) displays system-wide options as they are stored in the RACF database in the ICB (Inventory Control Block). This NEWLIST generates one entry per complex. A unique key is COMPLEX. This NEWLIST does not include an AUDITCONCERN field because the information is too extensive to report for the entire system. You can report on audit concerns using

the AUDIT NEWLIST. Unless otherwise noted, you can use all fields for SELECT and EXCLUDE processing as well as in the following output commands: LIST, SORTLIST, SUMMARY, and DISPLAY.

Field descriptions

The SETROPTS NEWLIST provides the following fields for reporting.

ADSP, SETRADSP, SYSTEMADSP

This RACF flag indicates whether Automatic Data Set Protection (ADSP) is in effect (due to a SETROPTS ADSP command). If set (ADSP=YES), RACF creates a discrete profile for each new data set created by users that have the ADSP attribute on their user profile or on their current connect group. If not set, individual user or connect group ADSP attributes are not honored. This field supports overtype.

AIM_DB_STAGE

This field contains the stage of implementation of the Application Identity Mapping feature of RACF.

APPLAUDIT

This RACF flag indicates whether APPC transactions will be audited through the APPL class. If set (APPLAUDIT=YES), APPC transaction start and end will be audited (if an APPL class profile is present and has success auditing specified). If not set, the APPC transaction start and end is not audited.

The option indicated by this flag can be set by a SETROPTS APPLAUDIT command. This field supports overtype.

AUDIT_GROUP

This flag indicates whether RACF is logging all RACF commands and DEFINE requests affecting profiles in the GROUP class. These commands are ADDGROUP, ALTGROUP, CONNECT, DELGROUP, and REMOVE. It reflects the SETROPTS AUDIT(GROUP) setting. This field supports overtype.

AUDIT_USER

This flag indicates whether RACF is logging all RACF commands and DEFINE requests affecting profiles in the USER class. These commands are ADDUSER, ALTUSER, CONNECT, DELUSER, PASSWORD and REMOVE. It reflects the setting SETROPTS AUDIT(USER). This field supports overtype.

BATCHALLRACF

This RACF flag indicates whether JES is only to accept jobs containing either a valid RACF userid and password or propagated RACF information. If set (BATCHALLRACF=YES), any job not containing this user identification fails. If not set, jobs without RACF userid runs with default authority, and have access according to UACC and the Global Access Table.

The option indicated by this flag can be set by a SETROPTS JES(BATCHALLRACF) command. This field supports overtype.

CATDSNS

This string indicates whether RACF prevents users from accessing uncataloged, new or system temporary data sets. It reflects an option set by a SETROPTS CATDSNS command. The following table documents the CATDSNS values, the corresponding SETROPTS commands, and their meanings.

Table 424. SETROPTS: CATSDNS values, associated SETROPTS command, and description

CATDSNS value	SETROPTS command	Meaning
No	SETROPTS NOCATDSNS	Uncataloged data sets are not protected from access
Warning	SETROPTS CATDSNS(WARNING)	Access to uncataloged data sets is allowed, but will result in a warning
Yes/Fail	SETROPTS CATDSNS(FAILURES)	Access to uncataloged data sets is only allowed to started tasks and SPECIAL users; access for other users will fail

This field supports overtype which means that authorized users can modify the field value through the ISPF interface.

CMDVIOL

This RACF flag indicates whether RACF is to log violations detected by RACF commands (due to a SETROPTS CMDVIOL command). If set (CMDVIOL=YES), command violations are logged. This field supports overtype.

COMPATMODE

This RACF flag indicates whether RACF is to allow users and jobs that do not have security labels on a system enforcing security labels (due to a SETROPTS COMPATMODE command). If set (COMPATMODE=YES), RACF allows users and jobs without security labels. This field supports overtype.

COMPLEX

The security complex name assigned to the security database. The complex name can come from the ALLOC COMPLEX parameter or default to a system name. It is the key for this record.

DASDVOL

This RACF flag indicates whether the DASDVOL class is active. If set (DASDVOL=YES), users that do not have ALTER access to a data set are still able to alter, rename, delete, dump and restore the data set if they have access to a profile in the DASDVOL class for the volume containing the data set.

Note: if DASDVOL is not active or if no profile covering the volume exists in the DASDVOL class, all users are granted access by DFDSS.

DLOGOPT

Auditing options for data sets (RACFclass=DATASET), due to a SETROPTS LOGOPTIONS command. The DLOGOPT values and the SETROPTS LOGOPTIONS auditing level are documented in the following table.

Table 425. SETROPTS: DLOGOPT values and associated SETROPTS LOGOPTIONS auditing level

DLOGOPT value	SETROPTS LOGOPTIONS auditing level
Always	ALWAYS
Failure	FAILURES
Never	NEVER

Table 425. SETROPTS: DLOGOPT values and associated SETROPTS LOGOPTIONS auditing level (continued)

DLOGOPT value	SETROPTS LOGOPTIONS auditing level
Profile	(determined by profile)
Success	SUCCESSES

Use the LOGOPT field of NEWLIST TYPE=CLASS to display auditing options for all classes.

EGN

This flag indicates whether Enhanced Generic Naming (EGN) is in effect (due to a SETROPTS EGN command). This field supports overtype.

ERASEONSCRATCH, EOS

String that indicates whether erase-on-scratch is in effect as a result of a SETROPTS ERASE command. If this option is in effect, data sets are physically erased when deleted or released for reuse. Table 426 lists the ERASEONSCRATCH values. Also see, the "ERASESECLEVEL" field.

Table 426. SETROPTS: ERASEONSCRATCH values and descriptions

ERASEONSCRATCH value	Meaning
All	All data sets are physically erased after delete as a result of a SETROPTS ERASE(ALL) command.
Lvl nnn	Physical erasure will be performed if the profile that protects the data set specifies ERASE or if the profile's security level is equal to or greater than the erase security level *nnn* as specified on the SETROPTS ERASE(SECLEVEL) command.
None	No data sets are physically erased after delete, even if the erase indicator in the data set profile is on (due to a SETROPTS NOERASE command).
Profile	The erase indicator in the data set profile is used to determine whether the data set is physically erased after delete (due to a SETROPTS ERASE(NOSECLEVEL) command).

Note: When migrated or backed up data sets are scratched from HSM owned DASD volumes, the field HSMERASE determines if HSM actually performs the erasure requested by the profile.

ERASESECLEVEL, SECLEVELERASE

String that indicates the security level at or above which all data sets are physically erased when deleted or released for reuse as a result of a SETROPTS ERASE(SECLEVEL) command. If the value is *None*, the ERASEONSCRATCH field determines erasure options. See "ERASEONSCRATCH." Otherwise, the value is a number representing the security level.

GENERICOWNER, GENOWN

Flag that indicates if restrictions on the creation of generic profiles are in effect as a result of a SETROPTS GENERICOWNER command. If the value is *Yes*, users can only create a generic profile more specific than any existing profile covering the same generic resource under the following conditions:

- The user has the SPECIAL attribute

- The user is the owner of the existing profile
- The profile is owned by a group and the user is group-SPECIAL in that group.
- The profile is owned by a user in a group and the current user is group-SPECIAL in that group.

This option does *not* apply to the class DATASET; for class DATASET, the CREATE authority determines who can create profiles. This field supports overtype.

GRPLIST, LISTGRP

This flag indicates whether list-of-groups processing is in effect (due to a SETROPTS GRPLIST command). If set (GRPLIST=YES), a user's authority to a resource is not based on the authority of the user's current connect group only, but on the highest authority of all groups the user is connected to. This field supports overtype.

HISTORY, PWDHISTORY

This string indicates the number of previous passwords stored by RACF (due to a SETROPTS PASSWORD(HISTORY) command). If set to '**No**', no password history is kept; otherwise, it contains a number in the range 1 to 32. This field supports overtype.

INACTIVE

This string indicates the number of days that a userid remains valid without being used (due to a SETROPTS INACTIVE command). If set to '**No**', users are never revoked because of lack of activity; otherwise, it contains a number in the range 1 to 255.

Note that inactive users are only revoked by RACF the next time user activity is attempted, for instance the next time the now inactive user tries to logon. Inactive users can be found using the CARLa script CKRLINAC. This field supports overtype.

INITSTATS

This flag indicates whether RACF statistics are updated by RACINIT processing (due to a SETROPTS INITSTATS command). This field supports overtype.

INTERVAL, PWDINTERVAL

This string indicates the maximum number of days a password remains valid (due to a SETROPTS PASSWORD(INTERVAL) command). If set to `No`, passwords never expire; otherwise, it contains a number in the range 1 to 254. This field supports overtype.

KERBLVL

This field contains the value of the SETROPTS KERBLVL setting, indicating the level of Kerberos support present on the system. It controls the types of encryption that can be used when setting up a Kerberos connection.

LVL1PREF

This string indicates whether RACF protection is in effect for data sets that have single-qualifier names (due to a SETROPTS PREFIX command). If set, it contains a 1- to 8-character first qualifier prefixed to the data set name to get the internal (resource) name. If empty, RACF protection for single-qualifier data sets is not in effect (due to a SETROPTS NOPREFIX command). This field supports overtype.

MINCHANGE

This field indicates the minimal number of days that must pass between a user's password changes (due to a SETROPTS PASSWORD(MINCHANGE()) command.) If set to '**No**', users can change their passwords more than once on the same day; otherwise, it contains a number in the range 1 to 254. This field supports overtype.

MIXEDCASE

This flag field indicates whether mixedcase passwords are used (due to a SETROPTS PASSWORD(MIXEDCASE) command.) This field supports overtype.

MLACTIVE

This string indicates whether RACF requires security labels to be present on all jobs, all resources defined in USER and DATASET, and all classes defined in the Class Descriptor Table (CDT) that require a security label. It reflects an option set by a SETROPTS MLACTIVE command. The following table documents the MLACTIVE values, the corresponding SETROPTS commands, and their meaning.

Table 427. SETROPTS: MLACTIVE values, corresponding SETROPTS commands, and descriptions

MLACTIVE value	SETROPTS command	Meaning
No	SETROPTS NOMLACTIVE	Security labels are not required
Warning	SETROPTS MLACTIVE(WARNING)	RACF allows jobs without a security label access to resources that do not have a security label, but issues a warning
Yes/Fail	SETROPTS MLACTIVE(FAILURES)	Security labels are required in all normal cases; privileged started tasks and SPECIAL users are allowed requests as long as data is not declassified

Classes in the Class Descriptor Table (CDT) that require a security label can be found using the SECLABEL field of NEWLIST TYPE=CLASS. This field supports overtype.

MLQUIET

This flag indicates whether RACF is to keep the system in a tranquil state (due to a SETROPTS MLQUIET command). If set (MLQUIET=YES), only started procedures, console operators, or SPECIAL users are able to logon, start new jobs, or access resources. This field supports overtype.

MLS

This string indicates whether RACF prevents users from declassifying data in a system using security labels. It reflects an option set by a SETROPTS MLS command. The following table documents the MLS values, the corresponding SETROPTS commands, and their meanings.

Table 428. SETROPTS: MLS values, corresponding SETROPTS commands, and descriptions

MLS value	SETROPTS command	Meaning
No	SETROPTS NOMLS	Users are allowed to declassify data
Warning	SETROPTS MLS(WARNING)	Users are allowed to declassify data, but any such action results in a warning
Yes/Fail	SETROPTS MLS(FAILURES)	Users are not allowed to declassify data

This field supports overtype.

MLSTABLE

This flag indicates whether the system has stabilized security labels (due to a SETROPTS MLSTABLE command). If set (MLSTABLE=YES), security labels can only be altered if MLQUIET is in effect. This field supports overtype.

MODELGDG

This flag indicates whether Generation Data Group (GDG) modeling is in effect (due to a SETROPTS MODEL(GDG) command). If set (MODELGDG=YES), the GDG base name, not the GDG generation name, is used to find the data set profile for the data set. This field supports overtype.

MODELGROUP

This flag indicates whether group modeling is in effect (due to a SETROPTS MODEL(GROUP) command). If set (MODELGROUP=YES), RACF uses a model profile to complete new group-named data set profiles. This field supports overtype.

MODELUSER

This flag indicates whether user modeling is in effect (due to a SETROPTS MODEL(USER) command). If set (MODELUSER=YES), RACF uses a model profile to complete new userid-named data set profiles. This field supports overtype.

NJEUSERID

This string indicates the userid to be used for SYSOUT or network jobs that are sent to the system without an RTOKEN or UTOKEN. The value of the string cannot be set to a userid defined in the RACF database.

The NJEUSERID can be set by a SETROPTS JES(NJEUSERID) command. The default value is a series of question marks (????????). This field supports overtype.

NOADDCREATOR

This flag indicates whether the system has to suppress the ALTER permit added by default to each newly created profile for the userid of the creator. This field supports overtype.

OPERAUDIT

This flag indicates whether RACF is logging all actions allowed only because a user has the OPERATIONS or group-OPERATIONS attribute. It reflects an option set by the SETROPTS OPERAUDIT command. This field supports overtype.

PRIMARY_LANGUAGE

This field indicates the RACF primary language setting as set by SETROPTR LANGUAGE(PRIMARY()).

PROTECTALL

This string indicates whether RACF protect-all processing is active (due to a SETROPTS PROTECTALL command). The following table documents the PROTECTALL values, the corresponding SETROPTS commands, and their meanings.

Table 429. SETROPTS: PROTECTALL values, corresponding SETROPTS commands, and descriptions

PROTECTALL value	SETROPTS command	Meaning
No	SETROPTS NOPROTECTALL	Users can access and create data sets that are not RACF-protected
Warning	SETROPTS PROTECTALL(WARNING)	Users can access and create data sets that are not RACF-protected, but any such action results in a warning
Yes/Fail	SETROPTS PROTECTALL(FAILURES)	Normal users are not allowed to access or create data sets that are not RACF-protected. Privileged started tasks and SPECIAL users are allowed to do so, but any such action results in a warning

This field supports overtype.

PWDRULE1

This string displays RACF password rule 1. RACF supports 8 different password rules, of which any one might be active or inactive (due to a SETROPTS PASSWORD(RULE)) command. If active, the password rule is of the form '**Length(min:max) Pattern**' or '**Length(max) Pattern**'. The Pattern is a string of **max** characters indicating what characters are valid at that position. The following table documents the possible character values and their meanings.

Table 430. SETROPTS: PWDRULE1 Character values and meanings

Pattern character	Meaning
*	Any character
$	National
A	Alphabetic
C	Consonant
c	Mixed consonant
L	Alphanumeric
m	Mixed numeric
N	Numeric
V	Vowel

Table 430. SETROPTS: PWDRULE1 Character values and meanings (continued)

Pattern character	Meaning
v	Mixed vowel
W	No vowel

Note that, when multiple password rules are active, RACF attempts to match a new password to *any* active rule, not *all* active rules. A password that is not accepted by one rule and accepted by another is therefore allowed by RACF.

PWDRULE2

This string displays RACF password rule 2. See the PWDRULE1 field.

PWDRULE3

This string displays RACF password rule 3. See the PWDRULE1 field.

PWDRULE4

This string displays RACF password rule 4. See the PWDRULE1 field.

PWDRULE5

This string displays RACF password rule 5. See the PWDRULE1 field.

PWDRULE6

This string displays RACF password rule 6. See the PWDRULE1 field.

PWDRULE7

This string displays RACF password rule 7. See the PWDRULE1 field.

PWDRULE8

This string displays RACF password rule 8. See the PWDRULE1 field.

RACFLEVEL, RACFLVL

A string that indicates the software level of RACF, for example: 'HRF7709'. This string is often tested by other products.

RACF_MLFSOBJ

This string indicates whether RACF requires security labels for files and directories. When the SECLABEL class is active, and MLFSOBJ is active, access to files and directories without security labels is denied except by trusted or privileged started tasks. Since HFS filesystems do not fully support security labels (except in read-only mode), conversion to zFS file systems is advisable before turning on this option. This field reflects the option set by a SETROPTS MLFSOBJ(ACTIVE|INACTIVE) command. This field supports overtype.

RACF_MLIPCOBJ

This string indicates whether RACF requires security labels for interprocess communications. When the SECLABEL class is active, and MLIPCOBJ is active, access to semaphores, message queues and shared memory without associated security labels is denied except by trusted or privileged started tasks. This field reflects the option set by a SETROPTS MLIPCOBJ(ACTIVE|INACTIVE) command. This field supports overtype.

RACF_MLNAMES

This string indicates whether the RACF name hiding function is in effect. This function has the following effects:

- Users cannot view the names of z/OS UNIX files and directories that their current security label does not give them authority to read.
- Users cannot view the names of data sets that a mandatory access check followed by a discretionary access check does not allow them to read.
- Users listing catalogs or directories cannot see the names of resources that they cannot currently read.
- Users cannot read a VTOC directly, unless they have been given authorization to the profile in the FACILITY class that protects the VTOC.

This field reflects the option set by a SETROPTS (NO)MLNAMES command. This field supports overtype.

RACF_SECLBYSYSTEM

This string indicates whether RACF allows security labels to be activated on a system image basis. When SECLBYSYSTEM is active, the SMF ID values specified in the member list of the profiles in the SECLABEL class will determine whether or not the security label is valid for each system. Security labels that are not valid for a system are considered inactive and cannot be used or listed by users without SPECIAL or AUDITOR on that system. This field reflects the option set by a SETROPTS (NO)SECLBYSYSTEM command. This field supports overtype.

REALDSN

This flag indicates whether RACF logging uses the real data set name (REALDSN=YES) or the naming-conventions name (REALDSN=NO) for logging purposes. It reflects an option set by the SETROPTS REALDSN command. This field supports overtype.

RETPD

This string specifies the RACF security retention period for tape data sets (due to a SETROPTS RETPD command). It is set to a number in the range 0 to 65533 for a tape data set that expires, and to 99999 for a tape data set that never expires. This field supports overtype.

REVOKE, PWDREVOKE

This string indicates the maximum number of consecutive invalid password attempts before a userid is revoked on the next invalid attempt (due to a SETROPTS PASSWORD(REVOKE) command). If set to '**No**', userids are never revoked because of invalid password attempts; otherwise, it contains a number in the range 1 to 254.

A REVOKE value of 5 means a userid is revoked at the *sixth* (not fifth) consecutive invalid password attempt. SPECIAL users are not revoked automatically after too many invalid password attempts. Instead, console message ICH301I is issued, and the operator must decide whether or not to revoke the SPECIAL user. This field supports the Overtype function which permits authorized users to edit the value from the ISPF interface.

RVARYSTATUSPWSET

This flag indicates whether the password for RVARY STATUS has been changed from the default value.

RVARYSWITCHPWSET

This flag indicates whether the password for RVARY SWITCH has been changed from the default value.

SAUDIT

This flag indicates whether RACF is logging all commands issued by users having the SPECIAL or group-SPECIAL attribute. It reflects an option set by the SETROPTS SAUDIT command. This field supports overtype.

SECLABELAUDIT

This flag indicates whether security label auditing is in effect (due to a SETROPTS SECLABELAUDIT command). If set (SECLABELAUDIT=YES), RACF uses the security label's auditing options in addition to the profile's auditing options for all access attempts. If no auditing options are set on the security label's profile, this option has no effect. This field supports overtype.

SECLABELCONTROL

This flag indicates whether security label control is in effect (due to a SETROPTS SECLABELCONTROL command). If set (SECLABELCONTROL=YES), the only users allowed to use the SECLABEL keyword of RACF commands are:

- SPECIAL users (all RACF commands)
- group-SPECIAL users (ADDUSER and ALTUSER commands)

If not set, all users with at least READ authority on the SECLABEL's profile can change profiles with this SECLABEL. This field supports overtype.

SECLEVELAUDIT

This string indicates whether security level auditing is in effect (due to a SETROPTS SECLEVELAUDIT command). If set to '**None**', auditing is not based on security levels; otherwise, it specifies the security level above which all access attempts are audited. This field supports overtype.

SECONDARY_LANGUAGE

This field indicates the RACF secondary language setting as set by SETROPTR LANGUAGE(SECONDARY()).

SESSIONINTERVAL, SESSINT

This string specifies the maximum session key interval that can be specified by RDEFINE or RALTER. It is set to a value in the range 1 to 32767 if session keys expire (SETROPTS SESSIONINTERVAL command); to '**None**' if no limit is set (due to a SETROPTS NOSESSIONINTERVAL command). This field supports overtype.

TAPEDSN

This flag indicates whether tape data set protection is in effect (due to a SETROPTS TAPEDSN command). If set (TAPEDSN=YES), RACF can protect tape data sets as well as tape volumes. This field supports overtype.

TAPEVOL

This flag indicates whether the TAPEVOL class is active.

If TAPEVOL is inactive, RACF is not able to guarantee the integrity of tapevolumes. Even if TAPEDSN is active, and even if you have a tape management system that assures 44 character data set name integrity (a tape only physically contains the last 17 in its data set header labels), it is still possible to circumvent security because of the fact that there is no protection between data sets on one tape. If you have access to one data set on a tape, you can use a non-APF-authorized program to access information of *all* data sets on the tape. So if you have TAPEVOL inactive, anyone can add an empty data set to that tape (unless it is completely full), and then access the other data sets.

The only way a tape management system can prevent this is by always checking access to the tape based on the first data set on the tape or by preventing multiple data sets on a tape.

Another protection that is inactive if TAPEVOL is off, is the protection against Bypass Label Processing (BLP). If TAPEVOL is off, no RACHECKS are done by DFP on the FACILITY profile ICHBLP.

TERMINAL

This flag indicates whether the TERMINAL class is active (due to a SETROPTS CLASSACT(TERMINAL) command).

TERMUACC

This string indicates the default universal access authority associated with undefined terminals (due to a SETROPTS TERMINAL command). It can have the values 'NONE' and 'READ'. This field supports overtype.

UNDEFINEDUSER

This string indicates the userid to be used for local jobs that enter the system without a userid; it might not be set to a userid defined in the RACF database.

The UNDEFINEDUSER can be set by a SETROPTS JES(UNDEFINEDUSER) command; the default is '**++++++++**'.

If a RACF version before 1.9 is used, this is set to '**n/a**'. This field supports overtype.

WARNING, PWDWARNING

This string indicates the maximum number of days before the expiration of a password, at which RACF is to issue a warning message to a user (due to a SETROPTS PASSWORD(WARNING) command). If set to '**No**', no warning is issued; otherwise, it contains a number in the range 1 to 255. This field supports overtype.

WHENPROGRAM, PROGRAM

This flag indicates whether RACF program control is active (due to a SETROPTS WHEN(PROGRAM) command). If set (WHENPROGRAM=YES), RACF protection is in effect for access to load modules and Program Control to Data Sets (PADS), independently of whether the PROGRAM class is active or not. This field supports overtype.

XBMALLRACF

This flag indicates whether JES2 is to test jobs to be run with an execution batch monitor for either a valid RACF userid and password or propagated RACF information. If set (XBMALLRACF=YES), all jobs not containing this user identification fail.

The option indicated by this flag can be set by a SETROPTS JES(XBMALLRACF) command. This field is modifiable.

SETROPTS_CLASS: RACF Class Settings in database

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The SETROPTS_CLASS NEWLIST (NEWLIST TYPE=SETROPTS_CLASS) lists class-specific SETROPTS options as they are stored in the RACF database ICB (Inventory

Control Block). Unless otherwise stated, all fields can be used for SELECT/EXCLUDE processing as well as in the output commands (LIST, SORTLIST, DISPLAY and SUMMARY).

It generates one entry per so-called POSIT value in the database; a unique key is COMPLEX POSIT. It is closely related to the NEWLIST TYPE=CLASS reports, in the sense that those display the incore settings from RCVT bits that supposedly should match those in the database. The main advantage of SETROPTS_CLASS over CLASS is that you do not need to have a CKFREEZE file with the proper content. This might be the case under VM, for instance, or if you are analyzing an old backup of a RACF database, or if you are analyzing the security of a system where you could not run zSecure Collect. Another advantage of SETROPTS_CLASS is that you do not see modifiable fields that in fact cannot be set independently since the classes have the same POSIT value. On the other hand, the advantage of TYPE=CLASS is that it combines the POSIT-based class settings with information from the CDT (Class Descriptor Table), like the actual class name. See "CLASS: RACF Class Descriptor Table" on page 989.

Class activity options for class DATASET do not have a POSIT number, but are nonetheless displayed. They can also be displayed with NEWLIST TYPE=SETROPTS as well. Note that site-defined classes will not display a class name, since there is no default class name for the site-defined POSIT values.

Field descriptions

The `SETROPTS_CLASS NEWLIST` provides the following fields for reporting.

ACTIVE

RACF protection for this class is active (due to a SETROPTS CLASSACT command). This field supports overtype.

AUDIT

Command auditing for this class is active (due to a SETROPTS AUDIT command). This field supports overtype.

AUDITCONCERN, CONCERN

This field returns a concatenation of audit concerns for the class. The following table shows the default audit priorities for active and non-active classes and the audit concerns. It is sorted by highest audit priority without a policy statement.

Table 431. SETROPTS_CLASS: audit priorities and associated audit concern descriptions for active and non-active classes

Audit priority active class	Audit priority non-active class	Audit concern
25	15	GENCMD off but GENERIC on
15	2	GENCMD on but GENERIC off
15	2	Violations not logged - LOGOPTIONS(NEVER)
5.	1	SETROPTS GLOBAL inactive, but profile present

The priority is 40 higher if the concern is not compliant to the policy that has been selected. A priority of 0 means the concern is not issued unless the policy has explicitly been requested.

The following audit concerns have been defined:

GENCMD off but GENERIC on

For this class the generic command processing has been turned off, while the class is being used as a generic class. Newly created profiles would turn out to be DISCRETE profiles, even if they contain generic characters. This situation should not occur.

GENCMD on but GENERIC off

The creation and deletion of generic profiles is possible, but RACF does not use them for access control. This could lead to data that is unprotected against expectations. This situation is intended for use when migrating from discrete profiles to generic profiles.

Violations not logged - LOGOPTIONS(NEVER)

This is undesirable since violations would not be journalled to SMF. Journalling violations and follow up tracking is critical to securing the resources within an installation.

SETROPTS GLOBAL inactive, but profile present

This suggests that somebody wanted to add entries for this class to the global access table, but did not succeed in doing so.

AUDITPRIORITY

This field returns the audit priority for the profile. See field AUDITCONCERN for a table with the concerns and their priorities. The actual audit priority can be higher because of e.g. a SIMULATE POLICY C2 statement.

DEFAULT_CLASS

Most commonly used class name that is controlled by the current POSIT value, as documented by IBM. Note that site-defined classes will not display a class name, since there is no default class name for the site-defined POSIT values. The link between POSIT value and class name is not stored in the RACF database, but in a load module (the Class Descriptor Table). See NEWLIST TYPE=CLASS for the mapping that a specific system uses when deploying the database.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

DESCRIPTION

This 64 character field returns a short explanation of the purpose of the class.

GEN

This string is set to '**Discrete**' if generic profiles in this class are not checked, and is empty otherwise.

GENCMD

Generic profile command processing for this class is active (due to a SETROPTS GENCMD or a SETROPTS GENERIC command). This field supports overtype.

GENERIC

Generic profile checking for this class is active (due to a SETROPTS GENERIC command). This implies that generic command processing for this class is active. This field supports overtype.

GENLIST

This flag indicates that this class has been GENLISTed, for example, that generic profiles for this class are shared in-storage (due to a SETROPTS GENLIST command). If this flag is set, the RACLIST flag cannot be set. This field supports overtype.

GLB

String indicating global access checking activity. It is set to `Glob` if global access checking is active, and blank if global access checking is inactive.

GLOBAL

Flag indicating Global Access Checking activity. Undefined if no Global Access checking is allowed, set if Global Access checking is active, and not set if Global Access checking is inactive. This field supports overtype.

LOGOPT

Auditing options for this class, due to a SETROPTS LOGOPTIONS command. The LOGOPT values and the SETROPTS LOGOPTIONS auditing level are documented in the following table.

Table 432. SETROPTS_CLASS: LOGOPT values and associated SETROPTS LOGOPTIONS auditing levels

LOGOPT value	SETROPTS LOGOPTIONS auditing level
Always	ALWAYS
Failure	FAILURES
Never	NEVER
Profile	(determined by profile)
Success	SUCCESSES

This field supports overtype.

POSIT

Options set id. This is a number in the range 0 to 1023 identifying a set of SETROPTS options that govern the activity of this class and all other classes having the same POSIT value. Whenever a SETROPTS command is issued for any class with a specific POSIT value, it applies to all classes with that value.

PROTECT

This is a string summarizing the protection options for this class and is based on the ACTIVE and AUDIT flags. The PROTECT values and the related values of the ACTIVE and AUDIT flags are documented in the following table.

Table 433. SETROPTS_CLASS: PROTECT values and related ACTIVE and AUDIT flag values

PROTECT value	ACTIVE flag	AUDIT flag
Inactive	NO	-
Noaudit	YES	NO
(blank)	YES	YES

RACLIST

This flag indicates that this class has been RACLISTed, for example, that both generic and discrete profiles for this class are shared in-storage (due to a

SETROPTS RACLIST(class) command). If this flag is set, the GENLIST flag cannot be set. This field supports overtype.

STATS

Flag indicating whether statistics are collected for this class (due to a SETROPTS STATISTICS command). This field supports overtype.

SMF: SMF records

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•			•	•	•

This section documents the fields for NEWLIST TYPE=SMF. Most fields can be used for SELECT/EXCLUDE processing as well as in the output commands (LIST, SORTLIST, DISPLAY and (D)SUMMARY), but there are some exceptions that can only be used for SELECT/EXCLUDE, or can only be used for output. The exceptions are noted in the description of the fields.

Most fields are not found in all SMF record types. The description of each field notes in which SMF record types the field is found. in addition, the end of this section contains a cross-reference table of fields and SMF record types.

- "Field descriptions"
- "Supported record types" on page 1388

Field descriptions

The `SMF NEWLIST` provides the following fields for reporting.

ACCESS

RACF allowed access. This field is found only in RACF processing records (SMF record types 80 and 83 subtype 1) written for a RACHECK (EVENT=ACCESS). Access granted through the global access table is not logged in this way.

Possible ACCESS values are documented in Table 434(increasing sort order).

Table 434. SMF record ACCESS field - available values

ACCESS value
N/A
NONE
EXECUTE
READ
UPDATE
CONTROL
ALTER
OWNER

The value N/A indicates that the preceding security label check already failed, so that the access level is not the cause of the failure

ACTION

The Action field is the action which caused the record to be created. This field is supported for the following SMF record types:

- DFSMS Statistics and Configuration records (SMF record type 42)
- INPUT (SMF record type 14)
- OUTPUT Data Set Activity (SMF record type 15)

For DFSMS Statistics and Configuration records, subtype 3 (SMF record type 42) Table 435 lists the possible action values. Only one value is returned.

Table 435. DFSMS Statistics and Configuration records - actions causing record creation

Record subtype	Actions that create records
3	ACTIVATE, ENF, VARY SMS, SAVEACDS
20	INITIALIZE
21	DELETE
22	ADD, CHANGE, DELETE
23	CREATE, EXTEND, UPDATE, READ, DELETE
24	ADD or REPLACE
25	RENAME
26	CREATE, REMOVE, RENAME

APPL

Application name as provided to RACF or the R_auditx service by the application. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) written for a RACINIT or RACHECK (EVENT=(RACINIT ACCESS)) and in R_auditx records (SMF record type 83 subtypes 2 and higher). It is also found in CICS records (SMF record type 110).

Note: This value of this field is determined by the application. It is not necessarily the same as the name of the application used for logging on.

AUTH_USER_HOSTNAME

This field is found in RACF processing and R_auditx records (SMF record type 80 and 83) and corresponds with RACF_SECTION(394) or RACF_SECTION(12), respectively. It contains the hostname cached by the Identity Context Extension (ICTX).

AUTH_USER_NAME

This field is found in RACF processing and R_auditx records (SMF record type 80 and 83) and corresponds with RACF_SECTION(392 or 424 if 392 is absent) or RACF_SECTION(10), respectively. It contains the authenticated user name cached by the Identity Context Extension (ICTX).

AUTH_USER_OID

This field is found in RACF processing and R_auditx records (SMF record type 80 and 83) and corresponds with RACF_SECTION(395) or RACF_SECTION(13), respectively. It contains the authentication object identifier cached by the Identity Context Extension (ICTX).

AUTH_USER_REGNAME

This field is found in RACF processing and R_auditx records (SMF record type 80 and 83) and corresponds with RACF_SECTION(393) or RACF_SECTION(11), respectively. It contains the registry name cached by the Identity Context Extension (ICTX).

BOX_SERIAL

This field describes the DASD unit volume serial number and device id for the data set. This field can be used to disambiguate between DASD volumes with the same VOLSER. See also "BOX_SERIAL field for DASDVOL report" on page 1014.

CATALOG

This field describes the catalog used. This field is found only in ICF processing records (SMF record types 36, 61, 65 and 66) and VSAM data set open and close records (SMF record types 62 and 64).

CERTIFICATE_ISSUER

This field is found in RACF processing records (SMF record type 80) and R_auditx records (SMF record type 83 subtypes 2 and higher) and corresponds with RACF_SECTION(332) or RACF_SECTION(2), respectively. If the user that caused this record to be written has authenticated himself to the system with a digital certificate, this field contains the distinguished name of the issuer of the certificate.

CERTIFICATE_LABEL

This repeated field is only found in RACF processing records (SMF record type 80) for RACDCERT events. It contains the certificate labels associated with this event. This field can contain up to 32 bytes of text, and is by default shown with that length.

CERTIFICATE_SERIAL

This field is only found in RACF processing records (SMF record type 80) and corresponds with RACF_SECTION(318). It contains the serial number of the certificate that is associated with this event. By default, this field is shown with a length of 10, though the contents can reach a length of 255 characters.

CERTIFICATE_SUBJECT

This field is found in RACF processing records (SMF record type 80) and R_auditx records (SMF record type 83 subtypes 2 and higher) and corresponds with RACF_SECTION(331), or RACF_SECTION(1) respectively. If the user that caused this record to be written has authenticated himself to the system with a digital certificate, this field contains the distinguished name of the subject of the certificate.

CICS_MONITOR_CLASS

For CICS monitoring records (SMF record type 110, subtype 1), this field returns the class of the monitoring record. The value is returned in decimal format. Table 436 provides a list of values and descriptions.

Table 436. CICS_MONITOR_CLASS - value

Value	Description
1	Dictionary record
3	Performance record
4	Exception record

Table 436. CICS_MONITOR_CLASS - value (continued)

Value	Description
5	Transaction resource record

The CICS_MONITOR_CLASS field is supported in both the super and sub records. The field is empty if the record is not a CICS monitoring record.

CICS_PERFORMANCE_DATA

For CICS Monitoring Performance class subrecords, (SMF 110, subtype 1, class 3), this field contains the field names and associated values for the CICS performance data stored in the record. The information reported is derived from the CICS data-dictionary and field connectors in the Performance Data section of the CICS monitoring record. If a performance data field does not contain a value, the field is not reported.

If the CICS record contains user-defined fields, the fields only display in the output if a dictionary has been read from SMF.

See the CICS monitoring facility documentation in the CICS Transaction Server for z/OS Information Center for more information: https://publib.boulder.ibm.com/infocenter/cicsts/v4r1/topic/com.ibm.cics.ts.home.doc/welcomePage/welcomePage.html.

CICS_SPECIFIC_APPL

For CICS monitoring records (SMF record type 110, subtype 1), this field identifies the specific CICS instance from which the data in the record was obtained. The value is derived from the CICS monitoring record field SMFMNSPN (Specific APPLID). Multiple CICS instances can be combined into a system using the generic APPLID name which is found in the APPL field.

CICS_TERM

This field returns the CICS terminal name associated with the transaction. This field is only supported for CICS monitoring performance sub records. (SMF 110 subtype 1, sub class 3). If this information is not available, this field is not reported.

CICS_TTYPE

For CICS monitoring performance subrecords, (SMF 110, subtype 1, class 3), this field returns a value indicating the type of transaction start (Start Code or Start Type). Table 437 shows the possible values for the CICS_TYPE field.

Table 437. CICS transaction start code or types

Value	Description
TO	The transaction was started (attached) by input of the transaction ID from the terminal user.
S	Attached by automatic transaction initiation (ATI) without data.
SD	Attached by automatic transaction initiation (ATI) with data.
QD	The transaction was started (attached) because the trigger level of an intrapartition transient data queue was reached.
U	The transaction was started (attached) by a CICS internal function generally as a result of some user request.
TP	Attached from terminal (TCTTE) transaction ID.

Table 437. CICS transaction start code or types (continued)

Value	Description
SZ	Attached by the Front End Programming Interface (FEPI).

If this information is not available, the field is not reported.

For information about transaction Start types, see the CICS-related SMF data section in the CICS Performance Analyzer for z/OS Report Reference.

CLASS

SAF class name. This field is found in the following record types:

- RACF processing and R_auditx records (SMF record types 80 and 83)
- Program signature verification records (SMF record type 86)

The CLASS field is derived for the following record types:

- SMF record types 14, 15, 17, 18, 30, 42, 60, 61, 62, 64, 65, and 66.
- HSM function statistics records.

For those SMF record types for which the SAF class is derived, the class is USER (for SMF record type 30), DATASET (when a resource name is found), or missing.

COMPCODE, COMPLETION_CODE

This field describes a job or step completion code. It is available in SMF record types 4, 5, and 30. It can describe a system abend code, a user abend code, or a return code (on successful completion). The COMPCODE field can have the following layouts:

Table 438. SMF record COMPCODE field - values for output processing

SELECT/EXCLUDE	Output code	Exploded output	Meaning
ACCESS RESOURCE	Ac	Resource	Access to the resource is being audited due to the AUDIT option, a logging request from the RACHECK exit routine, or because the operator granted access during *failsoft* processing
APPLAUDIT	Ap	Applaudit	Entity audited due to SETROPTS APPLAUDIT
CLASS	Cl	Class	SETROPTS AUDIT(class) - Changes to this class of profile are being audited
CMDVIOL	Vi	CmdViol	Violation detected in command and CMDVIOL is in effect
COMMAND ALWAYS	Cm	Command	RVARY or SETROPTS command issued: these commands are always audited
COMPATMODE COMPAT	Co	Compatmode	Entity audited due to SETROPTS COMPATMODE

Table 438. SMF record COMPCODE field - values for output processing (continued)

SELECT/EXCLUDE	Output code	Exploded output	Meaning
GLOBALAUDIT GLOBAL AUDITOR	G	Globalaudit	Access to entity being audited due to GLOBALAUDIT option
LOGOPTIONS	O	Logoptions	Class being audited due to SETROPTS LOGOPTIONS
NONE	blank	blank	No REASON value present in SMF record.
OMVS_AUTHORITY	Oa	OMVS authority	Audited because user does not have appropriate authority in OpenEdition MVS
OMVS_UNDEFINED	Ou	OMVS undefined	Audited because user not defined to OpenEdition MVS.
RACINIT	R	RACINIT failure	RACINIT failure
SECLABELAUDIT SECLABEL	Sl	Seclabel	Entity audited due to SETROPTS SECLABELAUDIT
SECLEVEL SECAUDIT	L	Seclevel	Entity audited due to SETROPTS SECLEVELAUDIT
SPECIAL	Sp	Special	SPECIAL or OPERATIONS users being audited (due to SETROPTS SAUDIT or SETROPTS OPERAUDIT).
USER	U	User	User being audited (due to ALTUSER UAUDIT)
VMEVENTVMAUDIT	Vm	VM event	VMEVENT auditing

Note: For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can come from the ALLOC COMPLEX parameter or default to a system name.

COMPSTAT, COMPLETION_STATUS

This field describes a job or step completion status. It is available in SMF record types 4, 5, 30, and 110 subtype 1, class 3 (CICS monitoring records performance class data). It can have the values described in Table 439 on page 1282.

Table 439. SMF record COMPLETION_STATUS field descriptions

COMPSTAT value	Types	Explanation
ABEND	4, 5, 30	User or system abend
FLUSHED	4, 30	Job or step was flushed
RC<>0	4, 5, 30	Nonzero result code, but not abended or flushed

CSSMTP_BADSPOOLDISP
A field indicating what the CSSMTP application should do with a JES spool file in case errors were encountered when processing the spool file. The field can have one of the following values:

- *Hold* Change the disposition of the spool file to HOLD so that CSSMTP cannot process it.
- *Delete* Delete the bad spool file.

The bad spool file disposition field reflects the value of CSSMTP configuration statement BadSpoolDisp parameter.

CSSMTP_DATETIME

Date and time when the reader recognized the JOB card for the CSSMTP job.

CSSMTP_EXTWRTNAME
External writer name, identifying the instance of CSSMTP which wrote the SMF record. The extermal writer name field reflects CSSMTP configuration statement ExtWrtName parameter, or, if there is no such statement, it reflects the CSSMTP job name.

CSSMTP_ CKPFILE
Name of the file where checkpoint information is saved.

CSSMTP_CN_ESMTP
The type of the server associated with the connection. The field can have one of the following values:

- *SMTP* indicates it is an SMTP server.
- *ESMTP* indicates it is an ESMTP (Extended SMTP) server.

CSSMTP_CN_FIPS140
Flag field indicating whether the connection is on FIPS compliance level 140.

CSSMTP_CHECKPOINTING
Specifies how the CCSMTP checkpoint records are used when CCSMTP starts. The field value is only available if the CSSMTP start option *-f* has been specified and the CSSMTP started procedure includes a CHKPOINT DD statement. This field can have the following values:

WarmStart
Indicates that checkpoint records are employed to restart JES spool files at their last known status when CSSMTP restarts

ColdStart
Indicates that any checkpoint records from the previous run of CSSMTP are flushed when CSSMTP restarts.

Unavailable
Indicates that checkpointing is not performed.

CSSMTP_CN_LOCAL_IP
Local IP address of a connection.

CSSMTP_CN_LOCAL_PORT
Local port of a connection.

CSSMTP_CN_REMOTE_IP
Remote IP address for a connection.

CSSMTP_CN_REMOTE_PORT
Remote port for a connection.

CSSMTP_CN_TLS_SSL_PROTO
AT-TLS SSL protocol employed with a connection. This field can have one of the following values:

- N/A Not applicable because TLS/SSL is not employed.
- *SSL2* SSL version 2
- *SSL3* SSL version 3
- *TLS1* TLS version 1 and
- *TLS1.1* TLS version 1.1

CSSMTP_CN_TLSNC
AT-TLS negotiated cipher employed with a connection.

CSSMTP_CONFIG_FILE
Name of the file with CSSMTP configuration statements.

CSSMTP_CONSOLE
Name of the console that issued the command.

CSSMTP_DEAD_LETTER_ACTN
The action CSSMTP should take when a dead letter is detected. The field can have one of the following values:

- *Delete* Do not save the dead letter to a z/OS UNIX file system.
- *Store* Store the mail message to the directory reported in the CSSMTP_DEAD_LETTER_DIR field

The CSSMTP_DEAD_LETTER_ACTN field returns the value from the CSSMTP configuration statement UNDELIVERABLE parameter DeadLetterAction.

CSSMTP_ DEAD_LETTER_DIR
This field represents the z/OS UNIX directory that CSSMTP uses for storing dead letters when the value of the CSSMTP_DEAD_LETTER_ACTN field is *Store*. The CSSMTP_DEAD_LETTER_DIR field reflects the value of the CSSMTP configuration statement UNDELIVERABLE parameter DeadLetterDirectory.

CSSMTP_DOMAIN_NAME
Domain Name used for a resolver MX query. This field reflects the value of the CSSMTP configuration statement TargetServer parameter TargetMx.

CSSMTP_HOST_NAME
Host name or fully qualified host name used for a resolver A or AAAA query. This field reflectsthe value of the CSSMTP configuration statement TargetServer parameter TargetName.

CSSMTP_LOGFILEC
CSSMTP client log file name.

CSSMTP_LOGLEVEL
The level of logging and tracing. The field reflects CSSMTP configuration statement LogLevel parameter.

CSSMTP_MAIL_ADMIN_MBOX
Repeated field with up to four e-mail addresses. These are the administrator

addresses to which CSSMTP delivers reports for certain errors. If the field is empty, no e-mail addresses have been configured to send a report. Each field value reflects the value of the CSSMTP configuration statement `MailAdministrator` parameter.

CSSMTP_MH_CMD_ERROR
Mail header text of command in error.

CSSMTP_MH_DATE
Mail header `Date` value.

CSSMTP_MH_ERROR_TEXT
Mail header error message text.

CSSMTP_MH_FROM
Mail header `Mail From` value.

CSSMTP_MH_MSGID
Mail header `Message-id` value.

CSSMTP_MH_RCPT_REPLY
Mail header `Reply to RCPT TO` value.

CSSMTP_MH_REPLY_TO_ERROR
Mail header text of reply to command in error.

CSSMTP_MH_SUBJECT
Mail header `Subject` value.

CSSMTP_MH_TO
Mail header `RCPT TO` value.

CSSMTP_REPORT
Action taken for reporting problems with JES spool files. The field can have one of the following values:

- *None* No error reports are created.
- *Admin* Error reports are sent to the configured mail administrators.
- *Sysout* CSSMTP creates a sysout file that contains the error report.

The field reflects the value of the CSSMTP configuration statement `REPORT` parameter.

CSSMTP_RTN_TO_MAIL_FROM
Flag field that indicates if CSSMTP sends an undeliverable mail notification to the originator when mail delivery fails. The field reflects the value of the CSSMTP configuration statement `UNDELIVERABLE` parameter `ReturnToMailFrom`.

CSSMTP_SMF119
Repeated field indicating which SMF type 119 subtype 48 to 52 records are written by CSSMTP.

- *Config* indicates configuration records (subtype 48) are written.
- *Connect* indicates connection records (subtype 49) are written.
- *Mail* indicates mail message records (subtype 50) are written.
- *Spool* indicates spool records (subtype 51) are written.
- *Stats* indicates statistical records (subtype 52) are written.

The absence of any of these values indicates that SMF type 119 records of the corresponding subtype are not written. The `CSSMTP_SMF119` field reflects the value of the parameters of the CSSMTP configuration statement `SMF119`.

CSSMTP_SI_SYSTEM
System name of the MVS image where the job output was created.

CSSMTP_SI_SYSTEM
System name of the MVS image where the job output was created.

CSSMTP_STACK
The name of the job employed to start the TCP/IP stack. In a common INET configuration, CCSMTP uses this job as a socket stack and for resolver functions. If CSSMTP_STACK is empty, the TCP/IP job name is either specified by the environment variable _BPXK_SETIBMOPT or no affinity is used in a common INET configuration.

CSSMTP_TS_DSTIP
Repeat group field. The IPv4 or IPv6 address of a target server to which CSSMTP connects. The value of the field reflects the CSSMTP configuration statement: TargetServer parameter, TargetName, TargetIP, or TargetMx.

CSSMTP_TS_INDEX
Repeat group field. Numerical field which indicates the order of the target server in the repeat group.

CSSMTP_TS_NAME
Repeat group field. The host name or fully qualified host name of a target server to which CSSMTP establishes a connection for sending mail. If the value of the CSSMTP_TS_TYPE field is *ADDRESS*, the value of the CSSMTP_TS_NAME field is a formatted IP address. The field reflects the value of the CSSMTP configuration statement TargetServer parameter TargetName, TargetIP, or TargetMx.

CSSMTP_TS_PORT
Repeat group field. The port that CSSMTP uses to connect to a target server. This port must match the listening port number used by the target server. The default port is 25. The field reflects the value of the CSSMTP configuration statement TargetServer parameter ConnectPort.

CSSMTP_TS_SECURE
Repeat group field. A flag field indicating whether Transport Layer Security (TLS) is required between CSSMTP and a target server. The field reflects the value of the CSSMTP configuration statement TargetServer parameter Secure.

CSSMTP_TS_TYPE
Repeat group field. Indicates the type of target server to which CSSMTP connects. The field indicates if the CSSMTP configuration statement TargetServer included a TargetName, TargetIP, or TargetMx parameter. The field can have one of the following values:

- *Address*. The CSSMTP configuration statement TargetServer included a TargetIP parameter.
- *Name*. The CSSMTP configuration statement TargetServer included a TargetName parameter.
- *MX*. The CSSMTP configuration statement TargetServer included a TargetMx parameter.

CSSMTP_USEID

User-defined identification field taken from the common exit parameter area, not from the USER=*parameter* on the job statement.

CSSMTP_USEREXIT
This field indicates whether CSSMTP calls the CSSMTP exit program to interrogate data that is sent to CSSMTP from the JES spool data set. If the

program is called, the field indicates which exit facility is used to call it. The field can have one of the following values:

- *NONE* Do not call the CSSMTP user exit.
- *VERSION2* Call the user exit using the exit facility token name EZBTCPIPSMTPEXIT.
- *VERSION3* Call the user exit using the exit facility token name EZATCPIPCSSMTPV3.

The field reflects CSSMTP configuration statement USEREXIT parameter.

DATASET, DSNAME, DSN

Data set name. This field is found in the following record types:

- Data set activity records (SMF record types 14, 15, 17, 18, 62 and 64)
- JES2 spool offload records (SMF record type 24)
- Catalog activity records (SMF record types 60, 61, 63, 65, 66, 67 and 68)
- RACF processing records (SMF record types 80 and 83 subtype 1)
- ACF2 data set use records
- TSS processing records (SMF record type 80)
- HSM function statistics records
- DB2 type 102 subtype/IFCid 34, 38, 39, 40, 104, 114, 119, 220, 258, and 362
- CSSMTP configuration records (SMF record type 119 subtype 48)
- DFSMS statistics and configuration records (SMF record type 42)

The DATASET field reflects the use of an actual data set. So RACF commands like PERMIT specifying a generic profile will NOT result in this field being filled. See also RESOURCE and PROFILE.

This is a repeated field, though only records describing a data set rename and some CSSMTP configuration records (SMF record type 119 subtype 48) contain more than one data set name

DATE

This field is present in all record types and contains the date the SMF record was written, in European format–08Oct2001 or 8 Oct 2001, for example. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see “Date fields” on page 903.

DATETIME

This field is present in all SMF records and contains both the date and time the record was written. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see “Combined date and time fields” on page 904.

DB2_APPL_USERID

This field contains the original application userid, as passed by Websphere Application Server, version 7.0. The default length of the field is 16, the maximum length 128. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but can cause information loss. The field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information. This processing behavior is the case for most subtypes.

DB2_AUTHID

This field contains the DB2 primary authorization id. This might or might not be identical to the USER field. Typically, the USER field is only filled in for some DB2 SMF record subtypes on a DB2 8.1 or higher system where DB2 is configured with a SAF interface, while the primary authorization id is always filled in. DB2 subsystem level tasks events often show SYSOPR as the primary authorization id. The default length for this field is 8, the maximum length is 128. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. The field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information. This processing behavior is the case for most subtypes.

DB2_COMMAND

This field contains a DB2 subsystem command (like -START TRACE or -STOP TRACE), or an SQL command. The default length of the field is 150, the maximum length 32760. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but can cause information loss. This field value is returned for SMF type 102 subtype/IFCid 4, 5, 63, 90, 92, 97, 140, 141, 142, 145, 270, 350, (if non-blank and not nulls).

DB2_CONNECTION

This field is meant to identify sequences of SMF records that apply to the same "session" connecting a user to DB2. These connections can take place through connection types like BATCH, IMS, TSO, and so on. The connection name is a readable string constructed from the following header fields in sequence as far as they are not the same value as already printed.

1. DB2 subsystem name (standard header),
2. DB2 location name (standard header),
3. network id (standard header),
4. LU name (standard header),
5. data sharing group name (data sharing header),
6. data sharing group member name (data sharing header),
7. connector type (correlation header),
8. connector name (correlation header),
9. original operator id (correlation header),
10. end-user workstation name (correlation header),
11. end-user transaction name (correlation header),
12. end-user userid (correlation header),
13. remote requestor location name (distributed header),
14. DRDA® server name (distributed header),
15. product name of application requestor (distributed header).

The default length of the field is 132. The maximum length is 32760. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. The field is filled in for SMF type 100, 101, and 102 if the standard header or optional correlation header section is present in the SMF record and the field contains non-blank, non-null information.

DB2_CONTEXT

This field contains the trusted context, which is a database security object. It can be used to establish a trust relationship between a DB2 database management system and an external entity, such as a middleware server. The default length of the field is 128, the maximum length 128. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. The field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information. This is the case for most subtypes.

DB2_ENDUSER_USERID

This field contains the DB2 end-user userid as passed to DB2. It is only present for certain types of remote access. The default length of the field is 16, the maximum length is 128. This field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information.

DB2_OBJECT

This repeating field contains a DB2 object name. The object type is provided by field DB2_OBJECT_TYPE, with a few exceptions. For example, names of a different type can be reported with type UserAuth, but this is what the SMF record says). Object names are often constructed as two level names like "owner.table" or "database.space". The default length for this field is 128, the maximum length is 257. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. This field is filled in for SMF type 102 subtypes/IFCids 6, 7, 8, 10, 22, 23, 24, 25, 62, 105, 107, 140, 142, 143, 144, 145, 177, 183, and 258, 271 if non-blank and non-null.

DB2_OBJECT_TYPE

This field contains the DB2 object type the event pertains to. Generally the object name is returned in field DB2_OBJECT, but there are some exceptions. For example, events pertaining to object type UserAuth are famous for containing object names of a different type. The default and maximum length of this field is 16. This field is filled in for SMF type 102 subtypes/IFCids 6, 7, 8, 10, 22, 23, 24, 25, 62, 105, 107, 140, 141, 142, 143, 144, 145, 177, 183, and 258, 271, 361, and 362.

DB2_ORIGINAL_OPERATOR

This field contains the DB2 Original Operator field. This is typically the userid submitting the work. If no real user can be identified, it is usually set to SYSOPR. The default length for this field is 8, the maximum length is 128. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. This field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information.

DB2_PLAN

This field contains the DB2 plan name active when the event occurred. The default and maximum length for this field is 8. This field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information.

DB2_ROLE

The field contains a DB2 role name. The role groups one or more privileges. Roles can be assigned to a primary authorization ID or to PUBLIC. The role is available only in a trusted context. The default length of the field is 20, the maximum length 128. This field can be in UTF-8. You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. The field is filled in for SMF type 100, 101, and 102 if the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information. This is the case for most subtypes.

DB2_SECAUTHID

This repeating field contains DB2 secondary authids. One of these IDs might be equal to the GROUP field, but typically the GROUP field is only filled in for some DB2 SMF record subtypes on a DB2 8.1 or higher system where DB2 is configured with a SAF interface. Most RACF interface authorization exits use the RACF connect groups as DB2 secondary authids. The default length for this field is 8, the maximum length is 128. This field can be in UTF-8.You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. This field is filled in for SMF type 102 subtype/IFCid 83 and 87 if non-blank and non-null.

DB2_SQLID

This repeating field contains DB2 SQL ids. If there are two, the first is the new and the second the old SQL id. The default length for this field is 8, the maximum length is 128. This field can be in UTF-8.You need an output file in UTF-8 encoding to be able to see all possible values. Conversion to EBCDIC is done when needed, but might cause information loss. This field is filled in for SMF type 102 subtype/IFCid 55, 83, and 87 if non-blank and non-null.

DESCRIPTOR, DESC

RACF descriptor. This field is found in RACF processing and R_auditx records (SMF record types 80 and 83). In addition, SUCCESS is emulated for job initiation and termination records (type 30), and WARNING is set for tape data set open and close records (type 14/15) in warning mode. This field is used to select records written for violations, warnings, undefined users, or successes. (Success is defined as the absence of a warning or violation.) When used for output, the default output is condensed; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 15, for example, DESCRIPTOR(EXPLODE,15). Table 440 shows the DESCRIPTOR values and their meaning.

Security zSecure emulates successful LOGON and LOGOFF events by using JOB INITIATION and JOB TERMINATION records. See 1290 for more information. DESC is always SUCCESS for these events.

Table 440. SMF record DESCRIPTOR, DESC - values for output processing

SELECT/EXCLUDE	Output code	Exploded output	Meaning
SUCCESS SUCCESSES	S	Success	The event is a success
UNDEFINEDUSER UNDEFINED	U	Undefined user	User is not defined to RACF
FAILURE VIOLATION VIOL	V	Violation	The event is a violation

Table 440. SMF record DESCRIPTOR, DESC - values for output processing (continued)

SELECT/EXCLUDE	Output code	Exploded output	Meaning
WARNING WARN	W	Warning	The event is a warning

Note: For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

DSTIP

Destination IP address. This field is found in z/OS Firewall Technologies records, SMF record type 109, SMF record type 118 (IPv4), SMF record type 119 (IPv6) and in EIM auditing records (type 83 subtype 2) where it is extracted from the EIM domain name. In record types 109, 118 and 119 it always is an IP address, in the EIM records it will mostly be a hostname.

DSTPORT

Destination port number. This field is found in z/OS Firewall Technologies records, SMF record type 109, SMF record type 118 (IPv4), SMF record type 119 (IPv6) and in EIM auditing records (type 83 subtype 2) where it is extracted from the EIM domain name.

ELAPSED

This field indicates the amount of time it took to run the transaction in TOD-clock format. It is supported in CICS SMF 110 records and subrecords (SMF 110 subtype 1, subclass 3).

ESM

This field contains the name of the External Security Manager, if known, or the text SAF. This field is filled in correctly if the program could match the SMF data set to an allocated CKFREEZE and UNLOAD or live security data base.

EVENT

The EVENT field describes the RACF event code. This field is only found in RACF processing records (SMF record types 80 and 83). When used in SELECT and EXCLUDE processing, this field is used to select both events and event qualifiers. For output, these fields are separated in EVENT and EVENTQUAL, while the output-only field EVENTDESC can be used to print a description of both event and qualifier.

When used for output, the EVENT field prints a string. Use the overriding type NUM to get the numerical event code.

For SELECT and EXCLUDE processing, each event type can be selected by number or symbolic name (for example, the RACINIT event type is also referenced as event number 1).

Starting with z/OS 1.7, a single event number can have multiple symbolic names, depending on the SMF record type and subtype. For example, the number 1 is a RACINIT event in type 80 and type 83 subtype 1, but in type 83 subtype 2 it is an EIMCONN event. It is therefore faster, and usually more accurate, to select on the symbolic name instead of on the numeric value. Each event type can be further specified by a sublist of *event qualifiers*. Event qualifiers are specified in a sublist, where a range of qualifiers can be specified using a colon (a range of events is not supported). Event qualifiers can also be specified using the symbolic values ALLOWED, SUCCESS, WARNING and FAILURE.

The following examples illustrate the syntax of the EVENT field.

Note: Only the =, <>, and ¬= relational operators can be used in SELECT and EXCLUDE statements.

```
SELECT EVENT=(PASSWORD, PERMIT, ADDSD)
SELECT EVENT=(RACINIT(1, 2, 3, 4, 5), RENAME(1))
SELECT EVENT=ALLCOMMAND(FAILURE)
SELECT EVENT=(APPCLU(FAILURE), 45(0, 1, 2), RACINIT(1:5, 8, 9))
SELECT EVENT<>(RACINIT(FAILURE) PASSWORD(ALLOWED))
```

Because RACF does not write SMF records for successful LOGON and LOGOFF events, Security zSecure emulates them from JOB INITIATION and JOB TERMINATION records (SMF type 30, subtypes 1 and 5). This emulation allows you to select and view all RACF LOGON and RACF LOGOFF events simply by selecting on RACINIT events.

The following sections provide reference information for the different types of event codes available for use in the SELECT and EXCLUDE statements.

- 1291
- 1291
- 1292
- 1293
- 1295

Symbolic event codes

In addition to the individual event codes defined in the following table, three symbolic *combination* event codes are defined:

Table 441. SMF record EVENT field - event code descriptions

Event code	Event type	Event numbers
ALLSVC	All RACF SVC events	1 through 7
ALLCOMMAND ALLCMD ALLCMDS ALLCOMMANDS	All RACF commands	8 through 25, 59, 66 and 78
ALLOMVS	All OpenEdition MVS events	28 through 58, 60 through 65, 75 through 77

Symbolic event qualifiers

The meaning of the symbolic event qualifiers is defined in the following table.

Table 442. SMF record EVENT field - symbolic event code descriptions

Symbolic qualifier	Meaning
ALLOWED	Successful and warning events: an action that succeeded
FAILURE VIOLATION	Failure event: the event did not succeed, but was a violation
SUCCESS	Success event: an action that succeeded without a warning
WARNING	Warning event: the event succeeded, but generated a warning

IBM Tivoli Key Lifecycle Manager event code descriptions

Table 443 lists the predefined Tivoli Key Lifecycle Manager event code (SMF record types 83, subtype 6) supported by Security zSecure. The first two columns list the events sorted by name. The second two columns show the same events sorted by event code. The event qualifier and descriptor text for these events are derived from the text in the SMF record.

Table 443. SMF record EVENT field - Tivoli Key Lifecycle Manager event code descriptions

Event Name	Event Code	Event Code	Event Name
TKLMAUTN	2	1	Unknown
TKLMAUTT	3	2	TLKMAUTN
TKLMAUTZ	4	3	TLKMAUTT
TKLMAUDI	6	4	TKLMAUTZ
TLKMCONF	7	5	TKLMSYNC
TKLMKEYR	8	6	TKLMAUDI
TKLMRESM	9	7	TLKMCONF
TKLMRUNT	10	8	TKLMKEYR
TKLMSYNC	5	9	TKLMRESM
UNKNOWN	1	10	TKLMRUNT

Predefined RACF and R_auditx event codes

Table 444 describes the predefined RACF and R_auditx event codes (SMF record types 80 and 83) supported by Security zSecure. The first two columns list the events sorted by name. The second two columns show the same events sorted by event code. For information on the event qualifiers for these event codes, see 1295.

Note: All event codes can also be selected by numerical value. The numerical values can also be used to select events that have not been predefined. This selection method can be useful when new event codes are introduced but are not yet supported by Security zSecure.

Table 444. SMF record EVENT field - predefined RACF and R_auditx event code descriptions

Name	Event code	Event code	Name
ACCESS	2	1	RACINIT
ADDGROUP	9	2	ACCESS
ADDSD	8	3	ADDVOL
ADDUSER	10	4	RENAME
ADDVOL	3	5	DELETE
ALTDSD	11	6	DELVOL
ALTGROUP	12	7	DEFINE
ALTUSER	13	8	ADDSD
APPCLU	26	9	ADDGROUP
CONNECT	14	10	ADDUSER
DEFINE	7	11	ALTDSD
DELDSD	15	12	ALTGROUP
DELETE	5	13	ALTUSER

Table 444. SMF record EVENT field - predefined RACF and R_auditx event code descriptions (continued)

Name	Event code	Event code	Name
DELGROUP	16	14	CONNECT
DELVOL	6	15	DELDSD
DELUSER	17	16	DELGROUP
GENERAL	27	17	DELUSER
initACEE	67	18	PASSWORD/PHRASE The PHRASE command is an alias of the PASSWORD command. These two commands are indistinguishable from each other in SMF. You can use SELECT EVENT=PHRASE as an alternative to SELECT EVENT=PASSWORD.
KTICKET	68	19	PERMIT
PASSWORD/ PHRASE	18	20	RALTER
PDACCESS	71	21	RDEFINE
PERMIT	19	22	RDELETE
PKIDPUBR	79	23	REMOVE
PTCREATE	82	24	SETROPTS
PTEVAL	81	25	RVARY
RACDCERT	66	26	APPCLU
RACINIT	1	27	GENERAL
RACLINK	59	59	RACLINK
RACPRIV	78	66	RACDCERT
RALTER	20	67	initACEE
RDEFINE	21	68	KTICKET
RDELETE	22	69	RPKIGENC
REMOVE	23	70	RPKIEXPT
RENAME	4	71	PDACCESS
RPKIEXPT	70	72	RPKIREAD
RPKIGENC	69	73	RPKIUPDR
RPKIREAD	72	74	RPKIUPDC
RPKIRESP	80	78	RACPRIV
RPKIUPDC	74	79	PKIDPUBR
RPKIUPDR	73	80	RPKIRESP
RVARY	25	81	PTEVAL
SETROPTS	24	82	PTCREATE

OpenEdition MVS event codes

Table 445 on page 1294 list the OpenEdition MVS event types supported by zSecure. The events are listed in ascending order by event code.

Table 445. SMF record EVENT field - OpenEdition MVS event code descriptions

Event code	Name
28	DIRSRCH
29	DACCESS
30	FACCESS
31	CHAUDIT
32	CHDIR
33	CHMOD
34	CHOWN
35	CLRSETID
36	EXESETID
37	GETPSENT
38	INITOEDP
39	TERMOEDP
40	KILL
41	LINK
42	MKDIR
43	MKNOD
44	MNTFSYS
45	OPENFILE
46	PTRACE
47	RENAMEF
48	RMDIR
49	SETEGID
50	SETEUID
51	SETGID
52	SETUID
53	SYMLINK
54	UNLINK
55	UMNTFSYS
56	CHKFOWN
57	CHKPRIV
58	OPENSTTY
60	CHK_IPC
61	MAKE_ISP
62	R_IPCntl
63	SETGRPS
64	CHKF2OWN
65	R_AUDIT
75	SETFACL
76	DELFACL
77	SETFSECL

Numerical event code qualifiers

The following tables list the numerical event qualifiers.

See the IBM publication *Security Server RACF Macros and Interfaces (SA22-7682)* for information on the numerical `eventqualifiers` that exist on your system for SMF record types 80 and 83.

Note: If IBM adds new event qualifiers not in these tables, Security zSecure handles them properly. Remember that symbolic qualifiers (FAILURE, WARNING, SUCCESS can also be used, and are usually preferable.

The following tables provide event qualifier information for the SMF record type 80 and 83 events.

Table 446. Event 1 qualifier codes and descriptions

Qualifier	Meaning
0	Successful start of job
1	Invalid password specified
2	The user is not a member of the used group
3	An invalid OIDCARD was used
4	The user is not authorized to the Port Of Entry
5	The user is not allowed to log on to the application specified
6	Access attempt by a revoked user
7	The RACINIT has automatically revoked the user because of excessive password and pass phrase attempts
8	Successful end of job
9	The userid specified is undefined
10	Insufficient SECLABEL authority
11	The user is not authorized to the SECLABEL specified
12	Successful verification of job or logon
13	End of job, or logoff
14	SETROPTS MLQUIET: user or job not allowed, system now requires more authority
15	RJE job not authorized
16	Surrogate job specified, but SURROGAT class not active
17	Surrogate job specified, and user not authorized to job
18	Surrogate job specified, and user not authorized to SECLABEL
19	User not authorized to job by JESJOBS class
20	Warning: insufficient SECLABEL authority
21	Warning: no SECLABEL specified

Table 446. Event 1 qualifier codes and descriptions (continued)

Qualifier	Meaning
22	Warning: the user is not authorized to the SECLABEL specified
23	The SECLABELS specified are not compatible
24	Warning: the SECLABELS specified are not compatible
25	The user's current password has expired
26	Invalid new password specified
27	Verification failed by installation exit ICHRIX01
28	Access attempt to revoked group-connect
29	An OIDCARD is required, but none was given
30	NJE job not authorized
31	Warning: unknown user propagated from trusted node
32	Successful logon using a PassTicket
33	Attempted logon using a replay of a PassTicket failed
34	Client `SECLABEL` not equivalent to servers
35	Userid automatically revoked due to inactivity
36	Invalid password phrase
37	Invalid new password phrase
38	Current password phrase has expired

Table 447. Event 2 qualifier codes and descriptions

Qualifier	Meaning
0	Successful access
1	Insufficient authority
2	Discrete profile not found
3	Warning: access only permitted because of warning mode on the profile
4	Access failed due to PROTECTALL
5	Warning: access only permitted because PROTECTALL was used in warning mode
6	Insufficient SECLEVEL or CATEGORY
7	Insufficient SECLABEL authority
8	Warning: SECLABEL required but not specified
9	Warning: Insufficient SECLABEL authority
10	Warning: Data set not cataloged
11	Data set not cataloged
12	Profile not found, resource class has RC>4.
13	Warning: Insufficient SECLEVEL or CATEGORY
14	Warning: no MAIN mode execution environment was present when using conditional access or an EXECUTE controlled program. Access granted due to ENHANCED-WARNING PGMSECURITY mode
15	A BASIC mode program used conditional access or an EXECUTE controlled program in ENHANCED PGMSECURITY mode

Table 448. Event 3 ADDVOL: Add and change volume qualifier codes and descriptions

Qualifier	Meaning
0	Successful processing of new volume
1	Insufficient authority to the profile
2	Insufficient SECLABEL authority
3	SETROPTS MLSTABLE: a less specific profile exists with a different SECLABEL

Table 449. Event 4: RENAME qualifier codes and descriptions

Qualifier	Meaning
0	Successful rename
1	Invalid HLQ specified for data set (not a user or group)
2	Data set renamed to a group data set, and user not in group
3	Insufficient authority
4	The discrete profile already exists
5	The naming convention exit has refused the userid
6	SETROPTS PROTECTALL: resource not protected
7	Warning: SETROPTS PROTECTALL: resource not protected
8	The second qualifier is not a userid
9	SETROPTS MLSTABLE: a less specific profile exists with a different SECLABEL
10	SETROPTS MLS: Insufficient SECLABEL authority
11	SETROPTS MLS: Old profile not protected by SECLABEL
12	SETROPTS MLS: New profile not protected by SECLABEL
13	SETROPTS MLS: New profile does not dominate old profile
14	Warning: SETROPTS MLS: Insufficient SECLABEL authority
15	Warning: SETROPTS MLS: Old profile not protected by SECLABEL
16	Warning: SETROPTS MLS: New profile not protected by SECLABEL
17	Warning: SETROPTS MLS: New profile does not dominate old profile

Table 450. Event 5: DELETE qualifier codes and descriptions

Qualifier	Meaning
0	Successful deletion of profile
1	Profile not found
Qualifier	Meaning
0	Successful deletion of volume
2	Invalid volume specified

Table 451. Event 6: DELVOL (delete one volume) qualifier codes and descriptions

Qualifer	Meaning
0	Successful deletion of volume.

Table 452. Event 7 DEFINE: Define resource qualifier codes and descriptions

Qualifier	Meaning
0	Successful definition of profile
1	Invalid HLQ specified for data set (not a user or group)
2	Data set renamed to a group data set, and user not in group
3	Insufficient authority
4	The discrete profile already exists
5	The naming convention exit has refused the userid
6	SETROPTS PROTECTALL: resource not protected
7	Warning: SETROPTS PROTECTALL: resource not protected
8	Warning: SETROPTS MLACTIVE: No SECLABEL specified
9	Warning: SETROPTS MLS: Insufficient SECLABEL authority
10	The second qualifier is not a userid
11	Insufficient SECLABEL authority
12	SETROPTS MLSTABLE: a less specific profile exists with a different SECLABEL

Table 453. ALLCMDS Events 8 - 25, 59, 78 qualifier codes and descriptions

Qualifier	Meaning
0	No violations detected
1	Insufficient authority to issue RACF command
2	Authority to issue RACF command, but keyword violations detected (partial update of the RACF database)
3	Successful retrieval of data set names affected by a security label change (only for DATASET commands)
4	System error retrieving data set names affected by a security label change (only for DATASET commands)

Table 454. Event 26 APPCLU: APPC session establishment qualifier codes and descriptions

Qualifier	Meaning
0	Successful session verification
1	Session established without verification
2	Local LU key will expire within 5 days
3	The partner LU access has been revoked, too many session key attempts failed
4	Partner LU key does not match local LU key
5	Session terminated because of LOCK keyword
6	Session key required but not defined
7	Possible security attack by partner LU
8	No session key defined for partner LU
9	No session key defined for local LU
10	SNA protocol error
11	Profile changed during verification
12	Local or partner session key has expired

Table 455. Event 27 General (application defined event): qualifier codes and descriptions

Qualifier	Meaning
0-99	Application-defined qualifier

Table 456. Events 28 – 30, 32 –37, 39 – 58, 60, 61 – 65, 75 – 77: ALLOMVS qualifier codes and descriptions

Qualifier	Meaning
0	No violations detected
1	Caller is not authorized to perform function
2	Security label failure

Table 457. Event 31: CHAUDIT qualifier codes and descriptions

Qualifier	Meaning
0	File's audit options changed
1	Caller does not have authority to change user audit options for this file
2	Caller does not have authority to change auditor audit options for this file
3	Security label failure

Table 458. Event 38 (INITOEDP (initialize z/OS UNIX process) qualifier codes and descriptions

Qualifier	Meaning
0	z/OS UNIX process successfully initialized
1	The user is not defined as UNIX user (no userid or no OMVS segment)
2	The user does not have a UID
3	The user's current connect group does not have a GID

Table 459. Event 59: Remote Sharing Facility RACLINK event qualifier codes and descriptions

Qualifier	Meaning
0	No violations detected
1	Insufficient authority to issue RACF command
2	Authority to issue RACF command, but keyword violations detected
3	Association was already defined
4	Association has already been approved
5	Association does not match
6	Association does not exist
7	No authorization to userid
8	Invalid password

Table 460. Event 61: MAKE_ISP qualifier codes and descriptions

Qualifier	Meaning
0	Successful creation of ISP

Table 460. Event 61: MAKE_ISP qualifier codes and descriptions (continued)

Qualifier	Meaning
1	Security label failure

Table 461. Event 67: INITACEE (certificate registration) qualifier codes and descriptions

Qualifier	Meaning
0	Successful certificate registration
1	Successful certificate deregistration
2	Caller is not authorized to register the certificate
3	Caller is not authorized to deregister the certificate
4	No user ID found for the certificate
5	The certificate is not trusted
6	Successful certificate authority certificate registration
7	Caller is not authorized to register the certificate authority certificate
8	The client SECLABEL is not equivalent to that of the server

Table 462. Event 68: KTICKET (Initial grant of Kerberos ticket) qualifier codes and descriptions

Qualifier	Meaning
0	Successful grant of Kerberos ticket
1	Failure to grant Kerberos ticket

Table 463. SMF record EVENT field - Event 69 qualifier codes and descriptions

Qualifier	Meaning
0	Successful certificate generation
1	Caller has insufficient authority to generate the certificate
2	Successful certificate generation request
3	Caller has insufficient authority to request generation of the certificate
4	Successful certificate renewal
5	Caller has insufficient authority to renew the certificate
6	Successful certificate renewal request
7	Caller has insufficient authority to request renewal of the certificate
8	Successful user preregistration
9	Caller has insufficient authority to preregister the user

Table 464. Event 70: RPKIEXPT (R_PKIServ EXPORT) qualifier codes and descriptions

Qualifier	Meaning
0	Successful certificate export
1	Caller has insufficient authority to export the certificate
2	Incorrect pass phrase specified

Table 465. Event 71: PDACCESS (Policy director access control decision) qualifier codes and descriptions

Qualifier	Meaning
0	Authorized to access object
1	Warning: Caller has insufficient authority to the object
2	Warning: Caller has insufficient traverse authority
3	Warning: Caller is not authorized due to a time-of-day check
4	Caller has insufficient authority to the object
5	Caller has insufficient traverse authority
6	Caller is not authorized due to a time-of-day check

Table 466. SMF record EVENT field - Event 72 qualifier codes and descriptions

Qualifier	Meaning
0	Successful admin QUERY or DETAILS request
1	Caller has insufficient authority for the admin QUERY or DETAILS request
2	Successful VERIFY request
3	Caller has insufficient authority for the VERIFY request
4	No record was found for the certificate in the VERIFY request

Table 467. Event 73: RPKIUPDR (R_PKIServUPDATEREQ) qualifier codes and descriptions

Qualifier	Meaning
0	Successful admin UPDATEREQ request
1	Caller has insufficient authority for the admin UPDATEREQ request

Table 468. SMF record EVENT field - Event 74 qualifier codes and descriptions

Qualifier	Meaning
0	Successful admin UPDATECERT request
1	Caller has insufficient authority for the admin UPDATECERT request
2	Successful REVOKE request
3	Caller has insufficient authority for the REVOKE request

Table 469. Event 79: PKIDPUBR (CRL publication) qualifier codes and descriptions

Qualifier	Meaning
0	Successful publication of Certificate Revocation List

Table 470. Event 80: RPKIRESP (R_PKIServRESPOND) qualifier codes and descriptions

Qualifier	Meaning
0	Successful RESPOND request
1	Caller has insufficient authority for the RESPOND request

Table 471. Event 81: PTEVAL (Passticket evaluation) qualifier codes and descriptions

Qualifier	Meaning
0	Successful passticket evaluation
1	Failure during passticket evaluation

Table 472. Event 82: PTECREATE (Passticket generation) qualifier codes and descriptions

Qualifier	Meaning
0	Successful passticket generation
1	Failure during passticket generation

Table 473. Event 83: RPKISCEP (R_PKIServSCEPREQ) qualifier codes and descriptions

Qualifier	Meaning
0	Successful AutoApprove PKCSReq request
1	Successful AdminApprove PKCSReq request
2	Successful GetCertInitial request
3	Rejected PKCSReq or CetCertInitial request
4	Incorrect SCEP transaction ID specified for GetCertInitial request
5	Caller has insufficient authority to issue a SCEPREQ request

Events defined for Event 83, subtype 2: EIM auditing

Table 474 lists the event codes for EIM auditing records. Each EIM event listed has a qualifier variable that returns event information. To see the possible values returned, see the table associated with each qualifier.

Table 474. Event 83, subtype 2: Events defined for EIM auditing (Record type 83 subtype 2) qualifier codes and descriptions

Event code	Event qualifier
1	EIMCONN (See Table 475.)
2	EIMLKUP (See Table 476 on page 1304.)
3	EIMSETUP (See Table 477 on page 1304.)
4	EIMADMIN (See Table 478 on page 1304.)

Complete information on the numerical event qualifiers that exist on your system for the different event types can be found in the Auditing chapter in the IBM publication *Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference*.

Table 475. Event 1: EIM Connection Event - qualifier codes and description

Qualifier	Meaning
0	Successful connect to the domain controller or a disconnection from the domain controller
3	Not authorized to connect to the domain controller

Table 476. Event 2 - EIM Lookup qualifier codes and descriptions

Qualifier	Meaning
0	Successful request
1	Insufficient authority to request EIM data
2	Mapping not found or the user was not authorized to access the EIM data

Table 477. Event 3: EIM Administrative Setup event - Domain, Registry, Access qualifier codes and descriptions

Qualifier	Meaning
0	Successful request
1	Unable to connect to the EIM domain
3	Insufficient authority to modify the EIM domain or retrieve information from the domain

Table 478. Event 4 - EIM Administrative - Identifiers, Associations, Policies qualifier codes and descriptions

Qualifier	Meaning
0	Successful request
1	Insufficient authority to modify the EIM domain or retrieve information from the domain

LDAP auditing records

The following tables lists the event codes for LDAP events recorded in the SMF data set. Each LDAP event listed has a unique event code with a corresponding event code qualifier variable that returns event information.

Table 479. SMF record, event 83, subtype 3: LDAP events

Event and meaning	Qualifier and meaning
1 - ADD operation	0 (Success), 1 (Failure)
2 - BIND operation	0 (Success), 1 (Failure)
3 - COMPARE operation	0 (Success), 1 (Failure)
4 - CONNECT operation	0 (Success), 1 (Failure)
5 - DELETE operation	0 (Success), 1 (Failure)
6 - DISCONNECT operation	0 (Success), 1 (Failure)
7 - EXTENDED operation	0 (Success), 1 (Failure)
8 - MODIFY operation	0 (Success), 1 (Failure)
9 - MODIFYDN operation	0 (Success), 1 (Failure)
10 - SEARCH operation	0 (Success), 1 (Failure)
11 - UNBIND operation	0 (Success), 1 (Failure)

Table 480. SMF record, event 83, subtype 4: R_AUDIT events

Event and meaning	Qualifier and meaning
1 - Authentication	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)
2 - Authorization	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)

Table 480. SMF record, event 83, subtype 4: R_AUDIT events (continued)

Event and meaning	Qualifier and meaning
3 - Auth mapping	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)
4 - Key management	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)
5 - Policy management	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)
6 - Admin config	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)
7 - Admin action	0 (Success), 1 (Info), 2 (Warning), 3 (Failure)

Signature verification auditing records

The following tables lists the event codes for signature verification auditing records. Each signature verification event listed has a qualifier variable that returns event information. To see the possible values returned, see the table associated with each qualifier.

Table 481. SMF record, event 86 (PSIGVER) signature verification qualifier codes and descriptions

Qualifier	Meaning
00	Successful signature verification.
01	Signature appears valid but root CA certificate not trusted.
02	Module signature failed verification.
03	Module certification chain incorrect.
04	Signature required by module not signed.
05	Signature required but signature has been removed.

EVENT_DATETIME

The EVENT_DATETIME field indicates the date and time of the transaction start. It has the same value as the DATETIME field. This field is only supported on CICS monitoring performance class subrecords (SMF subtype 1, subclass 3), The date is reported in local time.

EVENT_DATETIME_SMF

The EVENT_DATETIME field indicates the date and time of the transaction start. It has the same value as the DATETIME field. This field is only supported on CICS monitoring performance class subrecords (SMF subtype 1, subclass 3), The date is reported in local time.

EVENTDESC

The EVENTDESC field can only be used for output. It is found in the following records:

- Tivoli Key Lifecycle Manager audit security records (SMF record types 83, subtype 6)
- RACF processing and R_auditx records (SMF record types 80 and 83)

For Tivoli Key Lifecycle Manager audit security records, the event qualifier and descriptor text are derived from the text in the SMF record.

For RACF and R_auditx records, the field contains the name of the event, an indication of the result and a short explanation of the event qualifier, *Invalid password* for example.

The result field can be:

- **Success**
- **Warning**
- **Failure**
- **Undefined**

To print the numerical event qualifier, use the EVENTQUAL output field.

The default output length of this field is 64 characters. The full length can be up to 68 characters.

Note: The values printed by the EVENTDESC field are subject to change. Therefore, do not write applications that are dependent on the output of this field.

Security zSecure emulates successful LOGON and LOGOFF events by using JOB INITIATION and JOB TERMINATION records. See 1290 for more information.

EVENTQUAL

The EVENTQUAL field can only be used for output and is only found in RACF processing and R_auditx records (SMF record types 80 and 83). It can be used to print a numerical event qualifier. To print the event code, use the EVENT field described above; to print a description of the event and event qualifier, use the EVENTDESC field described above. To select records on event qualifier, use the EVENT field. The available event qualifiers are also listed with the EVENT field.

Security zSecure emulates successful LOGON and LOGOFF events by using JOB INITIATION and JOB TERMINATION records. See 1290 for more information. The event qualifiers are 0 and 8 for JOB INITIATION and JOB TERMINATION, respectively.

EXPLANATION

This field provides an additional description of a record and might indicate the cause of the record's creation. The field is only found in z/OS Firewall Technologies records (SMF record type 109) with message identifiers (MSGID) ICA1005e, ICA1032i, ICA1033i, ICA1034i, and ICA1035i.

FIELDVAL

This field can only be used for SELECT/EXCLUDE processing and is primarily meant for debugging purposes. It can also be used to select records by criteria not provided for by Security zSecure. FIELDVAL is used to select records that have specific values set at a specific offset. No equivalent output field exists.

The FIELDVAL field has the following syntax:
FIELDVAL=(offset in record,type,value) or
FIELDVAL=(offset in record,type,(list-of-values)). Both the offset and the values are in decimal; offset 0 indicates the start of the record (the length field). No relational operators other than = are allowed.

The following table describes the types supported:

Table 482. SMF FIELDVAL field - record types, descriptions and values

Type	Meaning	Values
BYTE	1-byte value	single or list
HALF	2-byte value	single or list
FULL	4-byte value	single or list

Table 482. SMF FIELDVAL field - record types, descriptions and values (continued)

Type	Meaning	Values
MASK1	1-byte bit mask (compare operation; the record is selected if any bit is set both in the record and in the bit mask)	single
MASK2	2-byte bit mask (compare operation; the record is selected if any bit is set both in the record and in the bit mask)	single

FILE

This field describes a ddname used by a program. It can be found in data set and activity records (SMF record types 14, 15, and 64), and ACF2 data set use records. These records also have a DATASET field; when both are used, the correspondence between ddname and data set name can be found.

GROUP

Group id. This field is found in the following record types:

- CICS monitoring records (SMF record type 110, subtype 1)
- For data set and ICF catalog activity records, it is derived using the job tag system (These records are SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65 and 66).
- CSSMTP client records (SMF record type 119) with subtype 48 if non-blank and non-null
- DB2 records (SMF record type 102) with subtypes/IFCids 83, 87, 140, 142, 269, and 314 if non-blank and non-null.
- DFSORT records (SMF record type 16)
- Job Initiation and Accounting records (SMF record types 20, 30 and 32)
- HSM function statistics records
- RACF processing and R_auditx records (SMF record types 80 and 83)
- NFS audit statistics records (SMF record type 42, subtype 26)

To select a group id that is the target of a RACF command, use one of the RACFCMD_GROUP, RESOURCE or PROFILE fields instead. The GROUP field describes the current connect group of the RACF command-issuing user, not the target group.

HOSTNAME

TCP/IP host name. This field is only found in z/OS Firewall Technologies records (SMF record type 109).

INTENT

SAF intended access. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) written for a RACHECK (EVENT=ACCESS). Also, it is derived for data set or ICF catalog activity records, as shown in the following table.

Table 483. SMF INTENT field - SMF type, Subtype and descriptions

SMF Type	Subtype	Description	INTENT derived
14		INPUT or RDBACK Data Set Activity	READ
15		OUTPUT, UPDATE, INOUT or OUTIN Data Set Activity	UPDATE
17		Scratch Data Set Status	ALTER
18		Rename Data Set Status	ALTER
42	26	NFS audit statistics	ALTER
61		ICF Define Activity	ALTER
62		VSAM Component or cluster open	READ, UPDATE, or CONTROL (action-dependent)
64		VSAM Component or Cluster Status	READ, UPDATE, or CONTROL (action-dependent)
65		ICF Delete Activity	ALTER
66		ICF Alter Activity	ALTER
102	6, 7, 34, 35, 114, 115, 116, 117, 118, 144	DB2 audit reads	READ
	8, 9, 10, 32, 38, 39, 40, 41, 119, 120, 143, 258	DB2 audit writes	UPDATE
	62, 142	DB2 audit alters	ALTER
	140, 145, 220	DB2 audit	NONE, EXECUTE, READ, UPDATE, or ALTER Action dependent

Possible INTENT values are documented in the following table (increasing sort order).

Table 484. SMF INTENT field - possible values

INTENT value
NONE
EXECUTE
READ
UPDATE
CONTROL
ALTER
OWNER

Access granted through the global access table will not show for record type 8x, but will be available through the other types.

IP_AUTOLOG_JOBNAME

A Repeat group field. The IP_AUTOLOG_JOBNAME field contains the name of the job used for the PORT reservation statement. This value can be identical to the value in the IP_AUTOLOG_PROCNAME field, but for z/OS UNIX jobs that create listener threads, it is not. If IP_AUTOLOG_JOBNAME is missing, the job name is assumed to be the same as the value of the IP_AUTOLOG_PROCNAME field.

IP_AUTOLOG_OPTIONS

The IP_AUTOLOG_OPTIONS repeat group flag field provides information about the following IP autolog configuration settings.

DELAYSTART DVIPA
The AUTOLOG procedure starts after the TCP/IP stack has joined the sysplex group and has processed its dynamic VIPA configuration.

DELAYSTART TTLS
The AUTOLOG procedure starts after the Policy Agent has successfully installed the AT-TLS policy in the TCP/IP stack and AT-TLS services are available.

IP_AUTOLOG_PARMSTRING

A Repeat group field. The IP_AUTOLOG_PARMSTRING field provides the parameter string to be added following the `START procedure_name`, where *procedure_name* is the value is found in the IP_AUTOLOG_PROCNAME field.

IP_AUTOLOG_PROCNAME

A Repeat group field. The IP_AUTOLOG_PROCNAME field contains the name of a procedure that the TCP/IP address space should start.

IP_AUTOLOG_WAIT

A Repeat group field. The IP_AUTOLOG_WAIT field shows the number of minutes that TCP/IP should allow for a procedure to come down when, at startup, it is still active and TCP/IP is attempting to AUTOLOG the procedure again. This could happen if the procedure did not come down when TCP/IP was last shutdown. When the IP_AUTOLOG_WAIT value is 0, TCP/IP startup does not cancel and restart any procedures in the autolog list that are already started. TCP/IP does not cancel the procedure at initialization. TCP/IP checks every 10 seconds (until the time interval specified by wait has expired) to check if the procedure has come down. If the procedure comes down during one of these 10 second intervals, it is restarted. If the procedure is still active when the time interval specified by wait expires, then TCP/IP cancels and restarts the procedure.

IP_CONFIG_CHANGES

IP_CONFIG_CHANGES is a repeated flag field that provides detailed information about IP configuration changes. Table 485 lists the fields that can be included in the IP_CONFIG_CHANGES field.

Table 485. IP_CONFIG_CHANGES field descriptions

Field	Description
DEP_INTERFACE	DEVICE, LINK, or BSDROUTINGPARMS statements were specified for non-strategic interface types.
DEP_HOME	HOME statements were specified for non-strategic interface types.
DEP_BEGINROUTES	GATEWAY or BEGINROUTES statements were used for non-strategic interface types.

Table 485. IP_CONFIG_CHANGES field descriptions (continued)

Field	Description
DEP_SMFCONFIG	Deprecated SMF statements, SMFPARMS, or SMFCONFIG 118 statements were specified.
DEP_TRANSLATE	TRANSLATE statements were specified for non-strategic interface types.
DEP_VIPASMPARMS	Deprecated
VIPADYNAMIC	VIPASMPARMS statements were specified.
CHANGED_AUTOLOG	An Autolog Procedure section was changed.
CHANGED_DV_ROUTES	A DVIPA Routes section was changed.
CHANGED_DIST_DV	A Distributed DVIPA section was changed.
CHANGED_IPV4	An IPv4 Configuration section was changed.
CHANGED_IPV6	An IPv6 Configuration section was changed.
CHANGED_TCP	A TCP Configuration section was changed.
CHANGED_UDP	An UDP Configuration section was changed.
CHANGED_GLOBAL	A Global Configuration section was changed.
CHANGED_PORT	A Port section was changed.
CHANGED_INTERFACE	An Interface / IPv4 addresses section was changed.
CHANGED_IPA6	An IPv6 addresses section was changed.
CHANGED_ROUTE	A Routes section was changed.
CHANGED_SRCIP	A Source IP section was changed.
CHANGED_MGMT	A Management section was changed.
CHANGED_IPSECCM	An IPSec Common section was changed.
CHANGED_IPSECRULE	An IPSec Default Rules section was changed.
CHANGED_NETACC	A Network Access section was changed.
CHANGED_DVIPA	A Dynamic VIPA (Virtual IP Address) Addresses section was changed.

IP_DATETIME_STARTED

The IP_DATETIME_STARTED field provides the date and time that the TCP/IP stack was started. The format of this field is DATETIME.

IP_DSNMEM

A Repeat group field. The IP_DSNMEM field contains a profile information entry for each data set name followed by a member name between brackets ([membername]). The data set name entries can originate from the following sources: an OBEYFILE command, the default library found in the standard search sequence, or an INCLUDE statement.

IP_DYNAMICXCF_INTFID

The IP_DYNAMICXCF_INTFID field specifies the interface ID which is used to form the link-local address for the interface. If this field is missing, TCP/IP generates a random value to be used to form the link-local address. The field value can be changed through the use of IPCONFIG6 statements.

IP_DYNAMICXCF_IP

The IP_DYNAMICXCF_IP field contains the IP address to be used as the home address for all dynamically generated XCF, Same Host, and HiperSockets links. The field value can be changed through the use of IPCONFIG statements.

IP_DYNAMICXCF_IPMASK

The IP_DYNAMICXCF_IPMASK field specifies the interface-level subnet mask for the IP_DYNAMICXCF link. If using OMPROUTE, this value is overridden with a corresponding OMPROUTE interface parameter value that can be coded or set to the default value. The field value can be changed through the use of IPCONFIG statements. If the destination address is IPv6, the IP_DYNAMICXCF_IPMASK field will be missing.

IP_DYNAMICXCF_IP6

The IP_DYNAMICXCF_IP6 field specifies the fully qualified IPv6 address that is used for all dynamically generated XCF, Same Host, and HiperSockets interfaces. The field value can be changed through the use of IPCONFIG6 statements.

IP_DYNAMICXCF_PFXLEN

The IP_DYNAMICXCF_PFXLEN field specifies the number of leftmost significant bits for the address mask. The field value can be changed through the use of IPCONFIG statements.

IP_DYNAMICXCF_PFXLEN6

The IP_DYNAMICXCF_PFXLEN6 field specifies the length of the routing prefix. If this field is not missing and if IP_DYNAMICXCF generates a HiperSockets interface definition, TCP/IP creates a prefix route over the HiperSockets interface using the number of bits specified in IP_DYNAMICXCF_PFXLEN6 of the IP_DYNAMICXCF_ADDRESS6. Therefore, you can configure other stacks outside the sysplex for the same IQD CHPID using IP addresses with the same prefix. This configuration automatically provides this stack with a route to the other stacks over the HiperSockets interface generated by IP_DYNAMICXCF. If IP_DYNAMICXCF_PFXLEN6 is missing, then TCP/IP does not create a prefix route over the HiperSockets interface. For interfaces other than HiperSockets which are generated from IP_DYNAMICXCF, the IP_DYNAMICXCF_PFXLEN6 value has no meaning. The field value can be changed through the use of IPCONFIG6 statements.

IP_DYNAMICXCF_SECCLASS

The IP_DYNAMICXCF_SECCLASS field specifies the security class for IP filtering associated with each dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. The value is used only when IPSECURITY is one of the values of the IPCONFIG field. Valid security classes are integers in the range 1 - 255. The default value is 255. The field value can be changed through the use of IPCONFIG statements.

IP_DYNAMICXCF_SECCLASS6

The IP_DYNAMICXCF_SECCLASS6 field specifies the security class for IP filtering with each IPv6 dynamic XCF interface. In order for traffic over the interface to match a filter rule, the filter rule must have the same security class value as the interface or a value of 0. The value is used only when IPSECURITY is one of the values of the IPCONFIG6 field. Valid security classes are integers in the range 1 - 255. The default value is 255. The field value can be changed through the use of IPCONFIG6 statements.

IP_DYN_XCF_SOURCEVIPAINT

The IP_DYN_XCF_SOURCEVIPAINT field specifies the name of the static VIPA interface used as the source IP address when SOURCEVIPA is one of the IPCONFIG6 values and outbound packets are sent over the dynamically generated XCF or Same Host interfaces.

IP_GLOBALCONF_IQDVLAN

The IP_GLOBALCONF_IQDVLAN field returns the VLAN ID which is used when HiperSockets (iQDIO) connectivity is used for dynamic XCF support. Valid VLAN IDs are integers in the range 1 - 4094. VLAN IDs are used to partition communication across HiperSockets. Stacks on the same CPC using the same HiperSockets CHPID that use the same VLAN ID can establish communications; stacks on the same CPC using the same HiperSockets CHPID that use different VLAN IDs cannot. The field value can be changed through the use of GLOBALCONFIG statements.

IP_GLOBALCONF_MLSCHKTERM

The IP_GLOBALCONF_MLSCHKTERM flag field indicates whether the stack should be terminated after writing an informational message when inconsistent configuration information is discovered in a multilevel-secure environment. The field value can be changed through the use of GLOBALCONFIG statements.

IP_GLOBALCONF_XCFGRPID

The IP_GLOBALCONF_XCFGRPID field provides a group ID value `tt` which is needed only if you want to use subplexing. If the field is not empty, *tt* is a two-digit suffix that is used in generating the XCF group name that the TCP/IP stack joins. The group name is `EZBT`*vvtt*, where the *vv* value is the VTAM XCF group ID suffix (specified with the XCFGRPID VTAM start option).

If no VTAM XCF group ID suffix was specified, the group name is `EZBTCP`*tt*.

If no VTAM XCF group ID suffix is specified and IP_GLOBALCONF_XCFGRPID is missing, the group name is `EZBTCPCS`.

These characters are also used as a suffix for the EZBDVIPA and EZBEPORT structure names, in the form `EZBDVIPA`*vvtt* and EZBEPORT*vvtt*. If no VTAM XCF group ID suffix was specified, the structure names are EZBDVIPA01*tt* and EZBEPORT01*tt*. If IP_GLOBALCONF_XCFGRPID is missing, the XCF group name is `EZBT`*vv*`CS` and the structure names are `EZBDVIPA`*vv* and `EZBEPORT`*vv*. If no VTAM XCF group ID suffix was specified, the group name is `EZBTCPCS` and the structure names are EZBDVIPA and EZBEPORT. The field value can be changed through the use of GLOBALCONFIG statements.

IP_INTERF_SOURCEVIPAINT

A Repeat group field. The IP_INTERF_SOURCEVIPAINT field has the name of the previously defined static VIPA interface which is used for SOURCEVIPA.

IP_INTERF_VMAC_ADDRESS

A Repeat group field. The IP_INTERF_VMAC_ADDRESS field contains the virtual MAC address. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv4 packets sent to and received from this TCP/IP stack. If VMAC_ADDRESS is missing, the OSA-Express device generates a virtual MAC address.

IP_INTERFACE_ASSOC_NAME

A Repeat group field. The IP_INTERFACE_ASSOC_NAME field provides the associated name for the interface, which can be the name for a Device, OSA-Express port, or TRLE definition depending on the interface type.

IP_INTERFACE_CHPID

A Repeat group field. The IP_INTERFACE_CHPID field provides the IQD Channel Path Identifier (CHPID) for the HiperSockets interface.

IP_INTERFACE_INDEX

A Repeat group field. The IP_INTERFACE_INDEX field provides the positive number assigned to the interface by the TCP/IP stack when the stack processed the configuration statement for the interface. The index value is used heavily by SNMP as the identifier of an interface for a stack because it is easier to use a number than a name.

IP_INTERFACE_INTERFACE

A Repeat group field. The IP_INTERFACE_INTERFACE field contains the name of an IPv4 or IPv6 interface.

IP_INTERFACE_INTFID

A Repeat group field. The IP_INTERFACE_INTFID field contains the configured interface ID. This ID is used to form the link-local address for the interface. The value is also appended to any manually configured prefixes for the interface to form complete IPv6 addresses on the interface.

IP_INTERFACE_IP

Repeat group field that provides the IPv4 and IPv6 addresses associated with the interface.

IP_INTERFACE_IPMASK

A Repeat group field. The IP_INTERFACE_IPMASK field provides the IPv4 subnet masks of the IPv4 addresses associated with the interface. For IPv6 addresses, the IP_INTERFACE_IPMASK field is empty, but not missing.

IP_INTERFACE_PFXLEN

Repeat group field that shows the prefix lengths for the subnet addresses of the IPv4 addresses, if any, associated with the interfaces.

IP_INTERFACE_OPTIONS

The IP_INTERFACE_OPTIONS repeat group flag field provides information about the settings for the IP stack interface configuration options. Table 486 lists the available configuration options.

Table 486. TCP/IP Interface Configuration settings

Option	Header
INTERFACE	The INTERFACE statement was employed (as opposed to DEVICE, LINK, or HOME statements).
AUTORESTART	In the event of a device failure, the TCP/IP address space attempts to reactivate the device.
NOAUTORESTART	For most device failures, the TCP/IP address space does not attempt to reactivate this device.
IPBCAST	The link both sends and receives IP broadcast packets.
MONSYSPLEX	Sysplex autonomics monitor the status of the link.
NOMONSYSPLEX	Sysplex autonomics do not monitor the status of the link.
DYNVLANREG	If a VLAN ID is configured for this link, it is dynamically registered with the physical switches on the corresponding LAN.

Table 486. TCP/IP Interface Configuration settings (continued)

Option	Header
NODYNVLANREG	If a VLAN ID is configured for this link, it must be manually registered with the physical switches on the corresponding LAN.
VMAC ROUTEALL	All IP traffic destined to the virtual MAC is forwarded by the OSA-Express device to the TCP/IP stack. If VMAC_ADDRESS is missing, the OSA-Express feature generates a virtual MAC address.
VMAC ROUTELCL	Only traffic destined to the virtual MAC and whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express. If VMAC_ADDRESS is missing, the OSA-Express feature generates a virtual MAC address.
CHECKSUM	Inbound checksum calculation is performed for all packets received on this interface.
NOCHECKSUM	Inbound checksum calculation is not performed for any packets received on this interface.
ISOLATE	OSA-Express is being prevented from routing packets directly to another TCP/IP stack that share the OSA. In this mode, OSA-Express discards any packets when the next hop address was registered by another stack that share the OSA. Packets can flow between two stacks that share the OSA only by first going through a router on the LAN.
NOISOLATE	Packets are routed directly between TCP/IP stacks sharing the OSA. In this mode, if the next hop address was registered by another stack that share the OSA adapter, then OSA-Express routes the packet directly to the sharing stack without putting the packet on the external LAN.

IP_INTERFACE_SECCLASS

A Repeat group field. The IP_INTERFACE_SECCLASS field provides the security class used for IP filtering with this interface. Valid security classes are integers in the range 1 - 255. The default value is 255.

IP_INTERFACE_TYPE

A Repeat group field. The IP_INTERFACE_TYPE field identifies the Interface type. Table 487 lists the available types.

Table 487. Possible values for the Interface type

Interface type	Description
LOOPBACK6	Loop back interface. One of the IPv6 addresses associated with the interface is `::1`. Additional loopback addresses can be defined.
IPAQENET	OSA-Express QDIO Ethernet, OSA-Express2, or OSA-Express3 interface for IPv4
IPAQENET6	OSA-Express QDIO Ethernet or Fast Ethernet interface for IPv6.
IPAQIDIO6	IPv6 HiperSockets interface.
MPCPTP6	MPC Point-To-Point Data Link Control interface. The interface can be used to carry IPv6 traffic over ESCON channels, over XCF links in a sysplex, or between z/OS Communications Server images using the simulated device provided by the IUTSAMEH function in VTAM.
VIRTUAL6 S	Static virtual interface for IPv6. The interface is not associated with real hardware and is used for fault tolerance support.

Table 487. Possible values for the Interface type (continued)

Interface type	Description
IPAQIDIO	MPCIPA for HiperSockets - Another TCP/IP within the same CPC.
MPCIPA for HiperSockets	Another TCP/IP within the same CPC.
MPCPTP	MPC Point-To-Point Data Link Control interface. The interface can be used to carry IPv4 traffic over ESCON channels or between z/OS Communications Server images using the simulated device provided by the IUTSAMEH function in VTAM.
VIRTUAL	Static virtual interface for IPv4. The interface is not associated with real hardware and is used for fault tolerance support.
LOOPBACK	Loop back interface. One of the IPv4 addresses associated with the interface is 127.0.0.1. Additional loopback addresses can be defined.

IP_INTERFACE_VLAN_ID

Repeat group field that contains the Virtual LAN identifier value. Valid VLAN IDs are in the range 1 - 4094.

IP_IPA6_INTERFACE_INDEX

Repeat group field that shows the numeric index value identifying an interface. SNMP often uses such index values because the index value is easier to reference than the interface name. An index value is assigned to an interface when processing a configuration statement for the interface.

IP_IPA6_INTERFACE_NAME

Repeat group field that contains the name of an IPv6 interface.

IP_IPA6_IP

Repeat group field that provides one of the IPv6 addresses associated with an interface.

IP_IPA6_PFXLEN

Repeat group field that shows one of the prefix lengths for the subnet address of one of the IPv6 addresses associated with the interface.

IP_IPCONFIG

The IP_IPCONFIG field is a repeated flag field that provides information about IPCONFIG parameters. The field value can be changed through the use of IPCONFIG statements. The field can have the following values:

CLAWUSEDOUBLENOP

Channel programs for CLAW devices are forced to have two NOP CCWs to end the channel programs. It is required for some vendor devices, and applies to only first-level MVS systems.

DATAGRAMFWD NOFWDMULTIPATH

The transfer of data between networks is enabled. When transferring data between networks, if there are multiple equal-cost paths to a destination, TCP/IP uses the first active route found for forwarding each IP packet.

DATAGRAMFWD FWDMULTIPATH PERPACKET

The transfer of data between networks is enabled. In transferring data between networks, if there are multiple equal-cost routes to a destination network or host, TCP/IP, upon forwarding an IP packet to a given host in that destination network, selects a route on an approximate round-robin basis from a multipath routing list to that destination host. The selected route is used for routing that IP packet. Connection or connectionless

oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NODATAGRAMFWD
The transfer of data between networks has been stopped by disabling IP datagram routing between different network interfaces. Forwarding is disabled.

DYNAMICXCF
Dynamic XCF support is enabled.

NODYNAMICXCF XCF
Dynamic support is not enabled.

FORMAT LONG
For stacks which are not enabled for IPv6, the command output is displayed as if it could contain IPv6 addresses. If the stack is enabled for IPv6, then the presence or absence of this value does not make any difference to the command format.

FORMAT SHORT
For stacks which are not enabled for IPv6, command output is displayed as if it could contain only IPv4 addresses and not the longer IPv6 addresses. If the stack is enabled for IPv6, this value is not present. This does not make any difference to the command format.

IGNOREREDIRECT
The IGNOREREDIRECT parameter was used in an IPCONFIG statement, or you are using OMPROUTE, or you are using Intrusion Detection Services (IDS) policy to detect and discard ICMP Redirects. As a result, TCP/IP ignores ICMP Redirect packets. IPSECURITY IPv4 IP filtering and IPv4 IPSec tunnel support are activated.

IQDIOROUTING
Inbound packets that are to be forwarded by the TCP/IP stack are eligible to be routed directly between a HiperSockets device and an OSA-Express device in QDIO mode without needing to be sent to this TCP/IP stack for forwarding. This type of routing over a HiperSockets device (iQDIO) is called HiperSockets Accelerator. If specified, HiperSockets Accelerator routes are created dynamically as this TCP/IP stack learns of destination IP addresses that can be routed to or from HiperSockets links without needing to be forwarded to this TCP/IP stack.

NOIQDIOROUTING
Inbound packets that are to be forwarded by this TCP/IP stack are not routed directly between a HiperSockets device and an OSA-Express device in QDIO mode. These packets are processed and routed by this TCP/IP stack.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled. In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERPACKET
Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host.

NOMULTIPATH
The multipath routing selection algorithm for outbound IP traffic is disabled. If there are multiple equal-cost routes to a destination, TCP/IP uses the first active route found to send each IP packet.

PATHMTUDISCOVERY
TCP/IP is to dynamically discover the PMTU, which is the smallest MTU of all the hops in the path. This is used to prevent fragmentation of datagrams.

NOPATHMTUDISCOVERY
TCP/IP is not to provide path MTU (PMTU) discovery support.

SOURCEVIPA
TCP/IP is to use the address present in the IP_TCPSTACKSOURCEVIPA field (if that field is not missing) or the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams that do not have an explicit source address. If the outgoing interface was defined with the INTERFACE statement, TCP/IP uses the VIPA specified on the SOURCEVIPAINTERFACE parameter of the INTERFACE statement instead of the HOME list.

NOSOURCEVIPA
TCP/IP is not to use the corresponding virtual IP address in the HOME list as the source IP address for outbound datagrams.

STOPONCLAWERROR
Channel programs (HALTIO and HALTSIO) are stopped when a device error is detected.

SYSPLEXROUTING
The TCP/IP host is part of an MVS sysplex domain.

NOSYSPLEXROUTING
The TCP/IP host is not part of an MVS sysplex domain.

QDIOACCELERATOR
Inbound packets that are to be forwarded by this TCP/IP stack are eligible to be routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface
- Two OSA-Express QDIO interfaces
- Two HiperSockets interfaces

These packets do not need to be sent to this TCP/IP stack for forwarding. This also applies to packets that would be forwarded by the Sysplex Distributor. This type of routing is called QDIO Accelerator.

NOQDIOACCELERATOR
Inbound packets that are to be forwarded by this TCP/IP stack are not routed directly between any of the following combinations of interface types:

- A HiperSockets interface and an OSA-Express QDIO interface.
- Two OSA-Express QDIO interfaces.
- Two HiperSockets interfaces

These packets are processed and routed by this TCP/IP stack.

IP_IPCONFIG6

The IP_IPCONFIG6 repeat group flag field provides information on the current settings for IPCONFIG6 parameters. Field value for these configuration settings can be changed through the use of IPCONFIG6 statements. Information on the following configuration settings can be included in this field.

DATAGRAMFWD NOFWDMULTIPATH
The transfer of data between networks is enabled. When transferring data between networks, if there are multiple equal-cost paths to a destination, TCP/IP uses the first active route found for forwarding each IP packet.

DATAGRAMFWD FWDMULTIPATH PERPACKET
The transfer of data between networks is enabled. In transferring data between networks, if there are multiple equal-cost routes to a destination network or host, TCP/IP, upon forwarding an IP packet to a given host in that destination network, selects a route on an approximate round-robin basis from a multipath routing list to that destination host. The selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same destination address do not always use the same route, but they do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NODATAGRAMFWD
The transfer of data between networks has been stopped by disabling IP datagram routing between different network interfaces. If the TCP/IP stack is also configured to be a sysplex distributor, datagrams destined to a sysplex-distributed dynamic VIPA are forwarded to stacks, whether or not forwarding is enabled.

DYNAMICXCF
Dynamic XCF support is enabled for IPv6.

NODYNAMICXCF
Dynamic XCF support is not enabled for IPv6 on this TCP/IP.

IGNOREREDIRECT
The IGNOREREDIRECT parameter was used in an IPCONFIG6 statement, or you are using OMPROUTE. TCP/IP ignores ICMPv6 Redirect packets.

IGNOREREDIRECT
The IGNOREREDIRECT parameter was used in an IPCONFIG6 statement, or you are using OMPROUTE. TCP/IP ignores ICMPv6 Redirect packets.

IGNOREROUTERHOPLIMIT
TCP/IP will ignore any hop limit value received in a router advertisement from a router. The global hop limit value (configured by way of IPCONFIG6 HOPLIMIT) is not overridden by the router advertisement value for all routes using the interface on which the router advertisement was received.

NOIGNOREROUTERHOPLIMIT
TCP/IP will not ignore a hop limit value received in a router advertisement from a router. This results in the configured global hop limit value being overridden by the router advertisement value for all routes using the interface on which the router advertisement was received.

IPSECURITY
IPv6 IP filtering and IPv6 IPSec tunnel support are activated.

MULTIPATH PERCONNECTION
The multipath routing selection algorithm for outbound IP traffic is enabled.

In general, multipath routing provides the routing distribution necessary to balance the network utilization of outbound packets by load splitting. Multipath routing requires multiple equal-cost routes that are either defined statically or added dynamically by routing protocols (except for RIP, which does not provide multipath routing). The MULTIPATH parameter has no effect if there are no multipath routes in the TCP/IP configuration.

MULTIPATH PERPACKET
Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. The selected route is used for routing that IP packet. Connection or connectionless oriented IP packets using the same source and destination address pair do not always use the same route, but do use all possible active routes to that destination host. All IP packets for a given association with a destination host are spread across the multiple equal-cost routes.

NOMULTIPATH
The multipath routing selection algorithm for outbound IP traffic is disabled. If there are multiple equal-cost routes to a destination, TCP/IP uses the first active route found to send each IP packet.

SOURCEVIPA
TCP/IP is to use a virtual IP address assigned to the IP_TCPSTACKSOURCEVIPA interface (if IP_TCPSTACKSOURCEVIPA is specified) or to the SOURCEVIPAINTERFACE interface as the source address for outbound datagrams that do not have an explicit source address. If multiple addresses are assigned to the IP_TCPSTACKSOURCEVIPA interface or the SOURCEVIPAINTERFACE interface, the source address is selected from among these addresses according to the default source address selection algorithm.

NOSOURCEVIPA
TCP/IP is not to use a VIPA address as the source IP address for outbound datagrams.

TEMPADDRS
TCP/IP is to generate IPv6 temporary addresses for PAQENET6 OSA-Express QDIO interfaces for which stateless address autoconfiguration is enabled.

NOTEMPADDRS
TCP/IP should not generate IPv6 temporary addresses.

IP_IPCONFIG_IPSECURITY

The IP_IPCONFIG_IPSECURITY flag field indicates whether IPv4 IP filtering and IPv4 IPSec tunnel support have been activated. The field value can be changed through the use of IPCONFIG statements.

IP_IPCONFIG6_IPSECURITY

The IP_IPCONFIG6_IPSECURITY flag field indicates whether IPv6 IP filtering and IPv6 IPSec tunnel support have been activated. The field value can be changed through the use of IPCONFIG6 statements.

IP_IPSEC_DVIPSEC

The IP_IPSEC_DVIPSEC flag field indicates whether IPsec tunnels associated with IPv4 dynamic VIPA addresses are eligible to be distributed if the dynamic VIPA address is being distributed. The IPsec tunnels are also eligible to be

moved during dynamic VIPA takeover or giveback. The field value can be changed through the use of IPSEC statements.

IP_IPSEC_LOGENABLE

The IP_IPSEC_LOGENABLE flag field indicates whether packet filter logging is enabled. If IP_IPSEC_LOGENABLE is true, then the following log messages might also be written to the syslog by the Traffic Regulation Manager Daemon (TRMD): EZD0814I, EZD0815I, EZD0821I, EZD0832I, EZD0833I, EZD0836I, and EZD0822I. The log setting on the individual default filter rules and the implicit default rules is honored. The field value can be changed through the use of IPSEC statements.

IP_IPSEC_LOGIMPLICIT

The IP_IPSEC_LOGIMPLICIT flag field indicates whether packet-filter logging is enabled for packets that are denied by the implicit default rules. IP traffic not explicitly permitted by the default IP filter rules parameters is handled by implicit default rules generated by the stack as long as the default IP filter policy is in effect. A setting of LOGIMPLICIT is honored only when filter logging is enabled on the IPSEC statement with LOGENABLE. The field value can be changed through the use of IPSEC statements.

IP_LAST_CHANGE_DATETIME

The IP_LAST_CHANGE_DATETIME field provides the date and time that the TCP/IP stack was last changed. The format of this field is DATETIME.

IP_NETACCESS_INBOUND

A repeat group field. IP_NETACCESS_INBOUND flag field indicates whether network access control checking is enabled for inbound socket commands.

IP_NETACCESS_IP

A repeat group field. IP_NETACCESS_IP field specifies an IP address or value that identifies the network or networks that require security product access control for user requests. The possible values are as follows:

IP address
Security product access control of user requests is required for the network with the specified IP address.

DEFAULT
Security product access control of user requests is required for any networks not specifically defined by other NETACCESS statement entries.

DEFAULTHOME
Security product access control of user requests is required for all IP addresses that are local to this stack and not specifically defined by other NETACCESS statement entries.

IP_NETACCESS_IPMASK

A Repeat group field. This field contains the IPv4 subnet mask. If the destination address is in IPV6 format, this field is missing.

IP_NETACCESS_OUTBOUND

A Repeat group field.This flag field indicates whether network access control checking is enabled for outbound socket commands.

IP_NETACCESS_PFXLEN

A Repeat group field. This field contains the prefix length of the Subnet address.

IP_NETACCESS_RACF_PROF

A Repeat group field. This field identifies the profile which protects the resource identified in the IP_NETACCESS_RESOURCE field. (See 1321.) The profile is simulated with the current RACF database.

IP_NETACCESS_RESNAME

A Repeat group field. This field contains the last qualifier of the resource name found in the IP_NETACCESS_RESOURCE field. (See 1321.) Effective user ids permitted to this resource are allowed to access the network.

IP_NETACCESS_RESOURCE

A Repeat group field. IP_NETACCESS_RESOURCE field identifies an SAF SERVAUTH resource. Effective user ids permitted to this resource are allowed to access the network. The resource looks like EZB.NETACCESS.sysname.tcpname.resname where

- *sysname* is the value of the MVS &SYSNAME. system symbol; it is present in the SYSNAME field.
- *tcpname* is the name of the procedure used to start the TCP/IP stack; it is present in the STACK field.
- *resname* is the 8-character value following the network specification in a NETACCESS statement. This value is present in the IP_NETACCESS_RESNAME field. (See 1321.)

IP_NETMON_PKTTRCSERVICE

The IP_NETMON_PKTTRCSERVICE flag field indicates whether the real-time TCP/IP packet trace service (SYSTCPDA) is enabled to run on the TCP/IP stack. This service enables network management applications to access trace data collected for any active packet traces or data traces. The field value can be changed through the use of NETMONITOR statements.

IP_NETMON_SMF_IPSECURITY

The IP_NETMON_SMF_IPSECURITY flag field indicates whether real-time IPSec SMF record support is enabled. The field value can be changed through the use of NETMONITOR statements.

IP_NETMON_SMF_PROFILE

The IP_NETMON_SMF_PROFILE flag field indicates whether real-time TCP/IP profile SMF event record support is enabled. The field value can be changed through the use of NETMONITOR statements.

IP_NETMON_SMFSERVICE

The IP_NETMON_SMFSERVICE flag field indicates whether the real-time SMF record information service (SYSCPSM) is enabled to run on the TCP/IP stack. The SMF record information service provides an interface for network management applications to obtain stack information in the form of SMF 119 records. Enabling or disabling this service has no effect on the SMF recording function that is available through separate configuration options on the SMFCONFIG profile statement or the FTP.DATA SMF configuration statements. The field value can be changed through the use of NETMONITOR statements.

IP_NETMON_TCPCONN_MINL

The IP_NETMON_TCPCONN_MINL field specifies the minimum connection lifetime, specified in seconds, for connections reported by the TCP connection information server. The server waits for this period before recording information about new connections; if the connection has closed in the meantime, then the

connection is not reported by the TCP connection information server. If the field contains 0, then all connections are reported. The field value can be changed through the use of NETMONITOR statements.

IP_NETMON_TCPCONNSERVICE

The IP_NETMON_TCPCONNSERVICE flag field indicates whether the real-time TCP connection information service (SYSTCPCN) is enabled to run on the TCP/IP stack. The TCP connection information service provides an interface for network management applications to obtain information about TCP connections on this stack. The field value can be changed through the use of NETMONITOR statements.

IP_PORT_BEGIN_PORT

A Repeat group field. The IP_PORT_BEGIN_PORT field contains the first port in a range of reserved ports. If missing in case UNRSV is true). The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_BIND

A Repeat group field. The IP_PORT_BIND field contains the IP address *ipaddr* which is associated with the job name present in the IP_PORT_JOBNAME field. When a job with the designated name IP_PORT_BINDs to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (`in6addr_any`), the IP_PORT_BIND is intercepted and converted to a IP_PORT_BIND to the IP address specified by *ipaddr*. Subsequent IP_PORT_BIND processing occurs as though the server instance had originally issued the IP_PORT_BIND to the IP address *ipaddr*. The field value can change through the use of PORT statements.

IP_PORT_END_PORT

A Repeat group field. The ENDPORT field contains the last port in a range of reserved ports. If the ports are not reserved (UNRSV= true), this field is missing. The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_JOBNAME

A Repeat group field. The IP_PORT_JOBNAME field specifies an MVS job name filter. If the value of the IP_PORT_PORT_USE field is *IP_PORT_JOBNAME*, then the IP_PORT_JOBNAME field indicates which job names can use the ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT range, or any unreserved port in case UNRSV is true. For multiple TCP reservations for the same port, or for multiple PORT UNRSV statements for the same protocol, the TCP/IP stack searches the PORT statements for the closest match (if any) to the application job name. The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_OPTIONS

The IP_PORT_OPTIONS repeat group flag field provides information about the current IP port configuration settings. Table 488 lists the settings that are reported.

Table 488. TCP/IP Configuration IP_PORT - Settings reported in IP_PORT_OPTIONS field

Option	Description
NOAUTOLOG	The TCP/IP address space is not to restart the server if it was stopped previously.

Table 488. TCP/IP Configuration IP_PORT - Settings reported in IP_PORT_OPTIONS field (continued)

Option	Description
DELAYACKS	Transmission of acknowledgments is delayed when a packet is received with the PUSH bit on in the TCP header. By default, this setting only affects connections that use a port in the specified port range. The behavior can be overridden by specifying the NODELAYACKS parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection: • The TCP/IP stack BEGINROUTES or GATEWAY profile statements • The Policy Agent RouteTable statement • The OMPROUTE configuration statements
NODELAYACKS	An acknowledgment is returned immediately when a packet is received with the PUSH bit on in the TCP header. Only connections that use this port are affected. Specifying the NODELAYACKS parameter on the IP_PORT_PORTRANGE statement overrides the specification of the parameter on the TCP/IP stack TCPCONFIG profile statement, or on any of the following statements used to configure the route used by the TCP connection: • The TCP/IP stack BEGINROUTES or GATEWAY profile statements • The Policy Agent RouteTable statement • The OMPROUTE configuration statements
SHAREPORT	TCP/IP allows multiple listeners to listen on the same combination of port and interface. Incoming connection requests for a port are distributed among the listeners using a weighted round-robin distribution method based on the server's accept Efficiency Fraction (SEFs) of the listeners sharing the port.
SHAREPORTWLM	TCP/IP allows multiple listeners to listen on the same combination of port and interface. The listener selection is based on WLM server-specific recommendations, modified by the SEF values for each listener.
DENY	Access to unreserved ports is denied. The IP_PORT_JOBNAME is an asterisk (*) in this case.
WHENLISTEN	Port access control is targeted to TCP applications acting as servers[10] that issue an explicit IP_PORT_BIND to a user-specified unreserved port. Permission to use the unreserved port is determined when a TCP `listen` command is issued. If a `listen` command is not issued, no access control check is made.
WHENIP_PORT_BIND	Permission to use an unreserved port is determined when an explicit IP_PORT_BIND to a specific local port is issued. For the UDP protocol, it can affect UDP applications that IP_PORT_BIND to a specific local port. For the TCP protocol, it can affect TCP client applications that IP_PORT_BIND to a specific local port for outbound connections.

IP_PORT_PORT_COUNT

A Repeat group field. The IP_PORT_PORT_COUNT field contains the number of ports in a range of reserved ports. If the ports are not reserved (`UNRSV= true`), this field is missing. The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_PORTRANGE

A Repeat group field. The IP_PORT_PORTRANGE field indicates whether a PORTRANGE statement was used (as opposed to a PORT statement). The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_PORT_USE

A Repeat group field. The IP_PORT_PORT_USE field indicates how the port is used.Table 489 lists the possible use types. The field value can change through the use of PORT and IP_PORTRANGE statements.

Table 489. TCP/IP Configuration IP_PORT: Port use types

Port use type	Meaning
RESERVED	The RESERVED field specifies that the ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT range (or all unreserved ports in case UNRSV is true) are not available for use by any user.
AUTHPORT	The AUTHPORT field specifies that all ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT port range (or all unreserved ports in case UNRSV is true) are not available for use by any user except FTP, and only when FTP is configured to use PASSIVEDATAPORTS.
IP_PORT_JOBNAME	The IP_PORT_JOBNAME field contains a filter indicating which job names can use the ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT range (or unreserved ports in case UNRSV is true).

IP_PORT_PROTOCOL

A Repeat group field. The IP_PORT_PROTOCOL field specifies the protocol associated with a range of ports. The value can be TCP or UDP. The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_RACF_PROFILE

A Repeat group field. The IP_PORT_RACF_PROFILE field identifies the profile which protects the IP_PORT_RESOURCE resource. The profile is simulated with the current RACF database. The field value can change through the use of the PORT and PORTRANGE statements.

IP_PORT_RESNAME

A Repeat group field. The IP_PORT_RESNAME field contains the last qualifier of the `SAF SERVAUTH` resource name present in the IP_PORT_RESOURCE field. All ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT port range (or all unreserved ports in case UNRSV is true) are reserved for users that are permitted to this resource. The field value can change through the use of PORT and PORTRANGE statements.

IP_PORT_RESOURCE

A Repeat group field. The IP_PORT_RESOURCE field provides the name of a SAF SERVAUTH resource. All ports in the IP_PORT_BEGIN_PORT to IP_PORT_END_PORT port range (or all unreserved ports in case UNRSV is true) are reserved for users that are permitted to this resource.

The field value can change through the use of PORT and PORTRANGE statements.

The following code shows a sample resource.

```
EZB.PORTACCESS.sysname.tcpname.resname
```

where

- *sysname* is the value of the `MVS &SYSNAME.` system symbol, which is present in the SYSNAME field.
- *tcpname* is the name of the procedure used to start the TCP/IP stack; it is present in the STACK field
- *resname* is the 8-character value following the SAF keyword in a PORT or PORTRANGE statement; it is present in the IP_PORT_RESNAME field.

IP_PORT_UNRSV

A Repeat group field. The IP_PORT_UNRSV flag field indicates whether a PORT UNRSV statement was used. Such statements indicate which applications or users are permitted to access application-specified unreserved ports. The following processing rules apply to PORT UNRSV statements:

- PORT UNRSV statements control access to all unreserved ports in the range 1 - 65535 unless RESTRICTLOWPORTS is configured. However, when RESTRICTLOWPORTS is configured, PORT UNRSV statements control access to unreserved ports above port 1023 only.
- For UDP, access control is applied when an application issues a bind to a particular port number to establish a local port. For TCP, access control is applied depending on the value of the WHENBIND or WHENLISTEN parameter.
- If neither DENY nor the SAF keyword is specified, an application that matches the protocol and specified job name [the job name can be an asterisk (*)] on a PORT UNRSV statement can access unreserved ports. If DENY is specified, all applications are denied access to unreserved ports for the specified protocol.
- If the SAF keyword is specified, applications that match the PORT UNRSV statement must also have user access to the SAF SERVAUTH resource which is indicated by the SAF keyword, to be permitted to access an unreserved port. The field value can change through the use of PORT statements.

IP_ROUTE_DSTIP

A Repeat group field. The DSTIP field specifies the destination IPv4 or IPv6 address. A DEFAULT keyword in this field specifies a default IPv4 route. A DEFAULT6 keyword in this field specifies a default IPv6 route. The field value can be changed through the use of BEGINROUTES statements.

IP_ROUTE_INTERFACE, IP_ROUTE_INTERFACE_INDEX

A Repeat group field. The IP_ROUTE_INTERFACE_INDEX or IP_ROUTE_INTERFACE field is a positive number assigned to the interface by the TCP/IP stack, when the stack processed the configuration statement for the interface. This number is used often by SNMP as the interface identifier for a stack because it is easier to use a number than a name.

IP_ROUTE_IPMASK

A Repeat group field. The IP_ROUTE_IPMASK field provides a BSD style address mask of an IPv4 destination address. The field value can change through the use of BEGINROUTES statements. For IPv6 addresses, the IP_ROUTE_IPMASK field is empty, but not missing.

IP_ROUTE_NEXTHOP_IP

A Repeat group field. The IP_ROUTE_NEXTHOP_IP field specifies the host IPv4 or IPv6 address of a gateway or router that you can reach directly, and that forwards packets for the destination network or host. The field value can change through the use of BEGINROUTES statements.

IP_ROUTE_PFXLEN

A Repeat group field. The IP_ROUTE_PFXLEN field specifies the number of mask bits for an IPv4 destination address or the prefix length for an IPv6 destination address. The field value can change through the use of BEGINROUTES statements.

IP_ROUTE_REPLACEABLE

The REPLACEABLE flag field indicates that the static route can be replaced by OMPROUTE and router advertisements when a dynamic route to the same destination is discovered.

IP_ROUTE_REPLACED

The REPLACED flag field indicates that the route is a replaceable static route that has been replaced by a dynamic route. The route is not currently being used by the TCP/IP stack.

IP_RULE_CODE

The IP_RULE_CODE field specifies the Internet Control Message Protocol (ICMP) code for IP traffic. This field is only applicable when the PROTOCOL is ICMP and the IP_RULE_TYPE field has a value other than asterisk (*). For IP traffic to be permitted by this rule, the ICMP code of the traffic must match the value in the CODE field. If the value of IP_RULE_CODE is asterisk (*), any ICMP code matches. See 1328.

IP_RULE_DSTIP

The IP_RULE_DSTIP field provides the destination IP address for the outbound rule. For outbound IP traffic to be permitted by this rule, the destination IP address of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the source IP address of the traffic must match this parameter.

IP_RULE_DSTIPMASK

A Repeat group field. The IP_RULE_DSTIPMASK field provides the destination IPv4 subnet mask. If the destination address is IPv6, this field is missing.

IP_RULE_DSTPFXLEN

A Repeat group field. The IP_RULE_DSTPFXLEN field provides the destination subnet address prefix length.

IP_RULE_DSTPORT

A Repeat group field. For TCP or UDP traffic, the IP_RULE_DSTPORT field specifies the destination port for the outbound rule and the source port for the generated inbound rule. Outbound traffic is permitted if the *destination port* matches this field value. Inbound traffic is permitted if the *source port* matches this field value.

IP_RULE_LOG

A Repeat group field. The IP_RULE_LOG flag field indicates whether packet-filter logging is enabled for the default filter rule.

IP_RULE_PROTOCOL

A Repeat group field. The IP_RULE_PROTOCOL field indicates the type of traffic that the rule applies to. For example, rules to permit or prevent IP traffic specify the protocol TCP. The IP_RULE_PROTOCOL field can have the following values: ICMP, TCP, UDP, ICMPV6, OSPF, and `nn`. The `nn` protocol specifies traffic that has number `nn`.

IP_RULE_ROUTING

A Repeat group field. The IP_RULE_ROUTING field indicates the type of packet routing that this rule applies to. Table 490 lists the available types.

Table 490. IP_RULE ROUTING field - available values

Routing value	Meaning
LOCAL	Indicates that this rule applies to packets destined for this stack.
ROUTED	Indicates that this rule applies to packets being forwarded by this stack.
EITHER	Indicates that this rule applies to both packets that are forwarded and those that are not forwarded.

IP_RULE_SECCLASS

A Repeat group field. The IP_RULE_SECCLASS field shows the Security class. The value can be an integer in the range 0 – 255 and has a default value of 0. A value of 0 matches any security class value coded on the corresponding profile statement which defines the interface.

IP_RULE_SRCIP

A Repeat group field. The IP_RULE_SRCIP field provides the source IP address for the outbound rule. For outbound IP traffic to be permitted by this rule, the source IP address of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the destination IP address of the traffic must match this parameter.

IP_RULE_SRCIPMASK

A Repeat group field. The IP_RULE_SRCIPMASK field provides the destination IPv4 subnet mask. If the source address is IPv6, this field is missing.

IP_RULE_SRCPFXLEN

A Repeat group field. The SCRCPFXLEN field provides the prefix length for the source subnet address.

IP_RULE_SRCPORT

For TCP or UDP traffic, the IP_RULE_SRCPORT field specifies the source port for the outbound rule. For outbound IP traffic to be permitted by this rule, the source port of the traffic must match this parameter. For inbound IP traffic to be permitted by the generated inbound rule, the destination port of the traffic must match this parameter.

IP_SACONF_SNMP_PWDEFAULT

The IP_SACONF_SNMP_PWDEFAULT flag field indicates whether the community name (or password) used to establish contact with an SNMP agent is `public`, which is the default. For the TCP/IP SNMP subagent to communicate with the z/OS Communications Server SNMP agent, the community name must match one that is defined in the PW.SRC or SNMPD.CONF data set used by the

SNMP agent or specified on the -c parameter when the SNMP agent is started. The field value can be changed through the use of SACONFIG statements.

IP_RULE_TYPE

The TYPE field specifies a value for the Internet Control Message Protocol (ICMP) type. Valid values are an asterisk (*) or in the range 0-255, The default is asterisk (*). This value is only applicable when the PROTOCOL is ICMP. For IP traffic to be permitted by this rule, the ICMP type of the traffic must match this parameter value. If TYPE=*, any ICMP type matches. (See also, 1326.)

IP_SMF119_FTPCLIENT

The IP_SMF119_FTPCLIENT flag field whether SMF type 119 records of subtype 3 are created when a user invokes the FTP client command. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_IFSTAT

The IP_SMF119_IFSTAT flag field indicates whether SMF type 119 records of subtype 6 containing statistics related to LINK utilization are created. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_IPSECURITY

The IP_SMF119_IPSECURITY flag field indicates whether SMF type 119 records of subtypes 77 and 78 are created when a dynamic tunnel is added and removed. Also, SMF type 119 records of subtypes 79 and 80 are created when a manual tunnel is activated or deactivated. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_PORTSTAT

The IP_SMF119_PORTSTAT flag field indicates whether SMF type 119 records of subtype 7 containing statistics related to reserved PORT utilization are created. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_TCPINIT

The IP_SMF119_TCPINIT flag field indicates whether SMF type 119 records of subtype 1 are created when TCP connections are established. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_TCPIPSTACK

The IP_SMF119_TCPIPSTACK flag field indicates whether SMF type 119 records of subtype 8 are created when a TCP/IP stack is activated and when it is terminated. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_TCPIPSTAT

The IP_SMF119_TCPIPSTAT flag field indicates whether SMF type 119 records of subtype 5 containing TCP/IP statistics are created. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_TCPTERM

The IP_SMF119_TCPTERM flag field indicates whether SMF type 119 records of subtype 2 are created when TCP connections are terminated. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_TN3270CLIENT

The IP_SMF119_TN3270CLIENT flag field indicates whether SMF type 119 records of subtype 22 and 23 are created when the TSO Telnet Client code starts or ends a connection. The field value can be changed through the use of SMFCONFIG statements.

IP_SMF119_UDPTERM

The IP_SMF119_UDPTERM flag field indicates whether SMF type 119 records of subtype 10 are created when a UDP Socket is closed. The field value can be changed through the use of SMFCONFIG statements.

IP_SYSPLEX_GROUP

The SYSPLEX field provides the group name for the sysplex.

IP_TCP_RESTRICTLOWPORTS

The IP_TCP_RESTRICTLOWPORTS flag field indicates whether TCP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements. In this case, applications that have a dependency on being able to obtain an available TCP port in the 1 - 1023 range without having that port explicitly reserved for its use should be run as APF authorized or superuser. The use of RESTRICTLOWPORTS increases system security. The field value can be changed through the use of TCPCONFIG statements

IP_TCPSTACKSOURCEVIPA

The IP_TCPSTACKSOURCEVIPA field specifies the IPv4 address used as the source IP address for outbound TCP connections. if SOURCEVIPA is one of the values of the IPCONFIG field. The address must be a static VIPA or an active dynamic VIPA (DVIPA). The field value can be changed through the use of IPCONFIG statements.

IP_TCPSTACKSOURCEVIPA6

The IP_TCPSTACKSOURCEVIPA6 field specifies the name of a static VIPA or a dynamic VIPA interface. If IP_SOURCEVIPA is one of the values of the IP_IPCONFIG6 field and if the interface has multiple IP addresses, then the *sourcevipa* address for outbound packets is selected from among these addresses according to the default source address selection algorithm. The field value can be changed through the use of IPCONFIG6 statements.

IP_UDP_RESTRICTLOWPORTS

The IP_UDP_RESTRICTLOWPORTS flag field indicates whether UDP ports 1 to 1023 are reserved for users by the PORT and PORTRANGE statements. In this case, applications that have a dependency on being able to obtain an available UDP port in the 1 - 1023 range without having that port explicitly reserved for its use should be run as APF authorized or superuser. The use of RESTRICTLOWPORTS increases system security. The field value can be changed through the use of UDPCONFIG statements.

IP_VIPA_ACTIVE

A Repeat group field. The IP_VIPA_ACTIVE field indicates whether the Dynamic Virtual IP (DVIPA) address is currently active.

IP_VIPA_INTERFACE

A Repeat group field. The IP_VIPA_INTERFACE field contains the name of the IPv6 interface.

IP_VIPA_IP

A Repeat group field. The IP_VIPA_IP field contains the Dynamic Virtual IP address (DVIPA).

IP_VIPA_IPMASK

A Repeat group field. The IP_VIPA_IPMASK field contains the IPv4 subnet mask. If the destination address is in IPV6 format, this field is missing.

IP_VIPA_PFXLEN

A Repeat group field. The IP_VIPA_PFXLEN field contains the prefix length of the Subnet address.

IP_VIPA_RACF_PROFILE

A repeat group field. This field identifies the profile that protects the resource identified in the IP_VIPA_RESOURCE field. The profile is programmatically derived using the current RACF database and RESOURCE as inputs.

IP_VIPA_RESNAME

A repeat group field. This field contains the last qualifier of the resource name found in the IP_VIPA_RESOURCE field. Effective user ids with at least READ access to this resource are allowed to:

- Create an application-specific DVIPA, specified by a specific VIPARANGE statement and by the SIOCSVIPA IOCTL call, the SIOCSVIPA6 IOCTL call, or the MODDVIPA utility.
- Delete a DVIPA that was created by using the same profile and the SIOCSVIPA IOCTL call, the SIOCSVIPA6 IOCTL call, or the MODDVIPA utility.

IP_VIPA_RESOURCE

A repeat group field. This field identifies an SAF SERVAUTH resource name. Effective user ids with at least READ access to this resource are allowed to:

- Create an application-specific DVIPA, specified by a specific VIPARANGE statement and by the SIOCSVIPA IOTCL call, the SIOCSVIPA6 IOTCL call, or the MODDVIPA utility.
- Delete a DVIPA that was created by using the same profile and the SIOCSVIPA IOTCL call, the SIOCSVIPA6 IOTCL call, or the MODDVIPA utility.

The SAF SERVAUTH resource name has the following format: `EZB.MODDVIPA.`*`sysname`*`.`*`tcpname`*`.`*`resname`*. The variable identifiers have the following meanings:

sysname is the value of the MVS `&SYSNAME.` system symbol. The value comes from the `SYSNAME` field.

tcpname is the name of the procedure used to start the TCP/IP stack. The value comes from the `STACK` field.

resname is the 8-character value following the `SAF` keyword in a `SAFNAME` statement. The value comes from the `IP_VIPA_RESNAME` field.

IP_VIPA_RANK

A Repeat group field. The IP_VIPA_RANK field specifies the intended order of the Virtual IP addresses in the VIPABACKUP statement. The VIPAs are listed in their respective backup chains, relative to other stacks in those backup chains. Larger numerical rank values move the respective stacks closer to the beginning

of the backup chain. Lower values indicate a position nearer to the end of the backup chain, while higher values indicate a position nearer to the beginning of the chain.

IP_VIPA_OPTIONS

The IP_VIPA_OPTIONS repeat group flag field provides information on the following configuration settings for the VIPA.

MOVEABLE IMMEDIATE
This value indicates whether the dynamic VIPA whose address is present in the IP field can be activated on this TCP/IP stack if the DVIPA is not already active elsewhere in the sysplex. If the DVIPA has been activated and the TCP/IP stack where the DVIPA is defined by a VIPADEFINE statement is subsequently activated, the DVIPA is activated immediately on that TCP/IP stack. The TCP connections to this TCP/IP stack are preserved. The MOVEABLE IMMEDIATE parameter is used only for activating the DVIPA when it is not already active in the sysplex. If the DVIPA is active, this parameter is ignored.

MOVEABLE NONDISRUPTIVE
Indicates an immediate, nondisruptive movement of a dynamic VIPA from one stack to another stack. A dynamic VIPA in the VIPARANGE statement can be moved to another stack when that stack requests ownership of the DVIPA as the stack creates it. This ownership request occurs under the following conditions:

- when an application binds to the DVIPA,
- when the MODDVIPA utility is used to create the DVIPA through the SIOCSVIPA or SIOCSVIPA6 ioctl
- when the application directly issues the SIOCSVIPA or SIOCSVIPA6 ioctl.

The new owning stack forwards packets for any existing connections to the original stack in order that the existing connections are not disturbed. All new connection requests are directed to the new owning stack.

CPCSCOPE
Indicates that the dynamic VIPA whose address is present in the IP field is specific to the central processor complex (CPC) on which it is defined. The VIPA is not moved to or taken over by another TCP/IP stack that is in a different CPC. A DVIPA defined with this characteristic can be used as the default route for incoming requests from Tier1 targets on this CPC. The Tier 1 target addresses must be on the same subnet as that determined by the address mask value present in the IP_VIPA_IP_VIPA_ field.

TIER1
The TIER1 field Indicates that the dynamic VIPA whose address is present in the IP field is used to distribute incoming requests to non-z/OS targets (for example, DataPower appliances or Linux hosts running on system Z).

TIER2
The TIER2 field indicates that the dynamic VIPA whose address is present in the IP field is used to distribute incoming requests from Tier1 targets to the group of server applications that is named.

SERVICEMGR
The SERVICEMGR field indicates that sysplex distributor performs Multinode Load Balancing (MNLB) by functioning as a Service Manager (in place of the Cisco LocalDirector). For these distributed dynamic VIPAs, SERVICEMGR has no effect if a VIPADISTRIBUTE DEFINE statement does not exist for the dynamic VIPA or VIPAs. SERVICEMGR is optional and can

be specified on a VIPABACKUP statement only when MOVEABLE is also specified. This parameter is used only for activating the DVIPA when it is not already active in the sysplex. If the DVIPA is active when the VIPABACKUP statement is processed, this parameter is ignored.

IP_VIPA_TYPE

A Repeat group field IP_VIPA_TYPE field identifies the Dynamic Virtual IP address (DVIPA) entry type. The following types are possible.

VIPABACKUP
This entry type designates one or more dynamic VIPAs for which this stack provides automatic backup.

VIPADEFINE
This entry type designates one or more dynamic VIPAs that this stack should initially own and support. Other stacks can provide backup for these VIPAs if this stack fails.

VIPARANGE
This entry type indicates whether a subnet for dynamic VIPA activation requests was honored through a BIND, SIOCSVIPA IOCTL, or SIOCSVIPA6 IOCT operation is to be defined or deleted. The value can be DEFINE or DELETE.

JOBCLASS

This field describes the JES job class in which the job generating the SMF record was running. It is a single character in the range A..Z, 0..9. This field is available in SMF record types 5 (Job Termination), 26 (JES Job Purge), and 30.

JOBELAPSED

Elapsed time for a job. This field is found in job termination records (SMF record type 5 and type 30, subtype 5). It indicates the time between the job start (for example, selected by an initiator) and the job end (the moment the job termination record was written). The time is indicated in minutes, rounded down; for example, SELECT JOBELAPSED<5 selects all job termination records with an elapsed time of up to 4 minutes, 59 seconds.

JOBID

This field provides the JES2 or JES3 jobid and can be found in the following record types:

- Accounting records (SMF record types 30 and 32).
- CICS monitoring records (SMF record type 110, subtype 1).
- For data set and ICF catalog activity records, it is derived using the job tag system (These records are SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65 and 66).
- CSSMTP client records (SMF record type 119) with subtypes 50 and 51 if non-blank and non-null.
- JES Job Purge records (SMF record type 26).
- RACF processing and audit records.
- Data sets and UNIX file system activity records (SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65, 66, 80, 83 and 92).
- CSSMTP mail and spool records (SMF record type 119, subtypes 50 and 51).

Depending on the record context, the value of JOBID can be in the following formats:

- Typical JES job: `J0Byyyyy`

- Started task control job: TSUyyyyy
- TSO/E user: STCyyyyy
- APPC/MVS transaction: Axxxxxxx

In these values, yyyyy and xxxxxxx are decimal numbers.

JOBNAME

Job or session name. This field is found in all job-related records.

The JOBNAME field is omitted if it is present in the record but only contains hex null characters. This most often occurs with TSO user logons (RACF processing records with EVENT=1) and with accesses during the logon process of a TSO user.

If the optional correlation header section is present in the SMF record and the field contains non-blank, non-null information, this field also available in the SMF record types: 100, 101, 102, and 110. It can also be found in CSSMTP client records (SMF record type 119) with subtypes 48, 49, 50, 51, and 52 if non-blank and non-null.SMF record types.

JOBTAG

The JOBTAG field is a compound field containing the information required to uniquely identify a job, for example, system id, jobname, reader date, and reader time. This field is found in all job-related records. It can be used for output only.

The job tag consists of 4 characters system id, 8 characters jobname, 11 characters reader date and 11 characters reader time, separated by spaces. The job tag for a job on system MLS1, with jobname SYSHSM, reader date 31 JAN 1994 and reader time 12:05:01.12 would be **'MLS1 31 JAN 1994 12:05:01.12 SYSHSM'**.

KEY_LABEL

Repeated field that contains the key labels associated with the event described by the SMF record. For record type 14, this field returns the values from the labels that identify the key for encrypting the data that was written to tape. For RACF processing records (type 80 and 83, subtype 1), this field contains the PKDS key label from relocate section 398. This field can contain up to 64 bytes of text, and is by default shown with that length.

KEY_LABEL_ENCODING

This repeated field contains the encoding for key label(s) associated with the event described by the SMF record. For record type 14, it is filled with either H or L, indicating Hash or Label encoding.

KEYRING_NAME

This field is only found in RACF processing records (SMF record type 80) and corresponds with RACF_SECTION(320). It contains the name of the keyring that is associated with this event. By default, this field is shown with a length of 64, though the contents can reach a length of 237 characters.

KERB_NAME

This field is only found in RACF processing records (SMF record type 80) and corresponds with RACF_SECTION(333). If the user that caused this record to be written has authenticated himself to the system using Kerberos, this field will contain the Kerberos principal name.

KERB_SOURCE

This field is only found in RACF processing records (SMF record type 80) and corresponds with RACF_SECTION(334). If the user that caused this record to be written has authenticated himself to the system using Kerberos, this field will contain the Kerberos login request source.

KERB_STATUS

This field is only found in RACF processing records (SMF record type 80) and corresponds with RACF_SECTION(335). If the user that caused this record to be written has authenticated himself to the system using Kerberos, this field will contain the Kerberos KDC status code.

LDAP_ENTRY_NM

This field is found only in LDAP R_auditx records (SMF record type 83 - subtype 3) and corresponds to RACF_SECTION(204). The field contains the target entry (for example, the Distinguished Name) of the operation: BIND, DELETE, ADD, and so on.

LDAP_CLIENT_SECL

This field is found only in LDAP R_auditx records (SMF record type 83 - subtype 3) and corresponds to RACF_SECTION(106). The field contains the LDAP client security label.

LDAP_CONN_ID

This field is only found in LDAP (R_auditx) records (SMF record type 83 - subtype 3) and corresponds to RACF_SECTION(103). The field contains an internal connection ID for the LDAP connection. The ID can be used to group operations performed on the same LDAP connection.

LOGSTR

SAF log string. This field is found in RACF processing and R_auditx records (SMF record type 80 and 83), ACF2 resource use, and ACF2 event records.

If you want to select records based on the contents of the log string, use the substring scan operator (`=:`) because a log string rarely contains a string at a fixed position. For example, to select all log strings with the word SDSF, use SELECT LOGSTR=:SDSF.

The default output length of LOGSTR is 64 characters; the full length might be up to 255 characters. To display the full LOGSTR in a column of limited width, use the WRAP output modifier, e.g. LOGSTR(WRAP,40). When LOGSTR reflects an executed CKGRACF command, and that command has more than 255 characters, part of the command is not present in LOGSTR. Devising a shorter REASON string will often help to limit the size of a CKGRACF command to 255 characters.

MEMBER

The `MEMBER` field returns the name of a member that has been changed. This field is supported in the following SMF record types:

- DFSMS statistics and configuration records (SMF record type 42, subtypes 21, 24, 25, and 26).
- `INPUT` or `RDBACK` Data Set Activity (SMF record type 14)
- `OUTPUT`, `UPDAT`, `INOUT`, or `OUTIN` Data Set Activity (SMF record type 15)
- TCP/IP profile event record (SMF record type 119, subtype 4)

For SMF records that are created by DFSMS Statistics and Configuration change or rename events (SMF record type 42, subtypes 14, 15, 21, 24, 25, and 26). This

field returns the name of a PDS or PDSE member that has been changed or renamed. The action that caused the change is reported in the ACTION field. (See 1276.)

For SMF type 119 subtype 4 and subtype 48 records, MEMBER is a repeated field. With each field entry is a member name which is found, between brackets, after a profile information data set name. The data set name can be found in the DATASET field. With SMF 119 subtype 4 records, thedata set followed by the member between brackets can be found in the IP_DSNMEM field. Each IP_DSNMEM entry was specified on an OBEYFILE command, or it is the default library found in the standard search sequence, or it was specified on an INCLUDE statement.

MEMBER_ALIAS

The MEMBER_ALIAS field only supported for SMF records created by DFSMS Statistics and Configuration Delete events (SMF record type 42, subtype 21). This field returns the names of aliases that were deleted when the PDSE member they were associated with (from the MEMBER field) was deleted.

MEMBER_OLDNAME

The MEMBER_OLDNAME field is only supported for SMF records created by DFSMS Statistics and Configuration Rename events (SMF record type 42 subtypes 25 and 26). The value returned is the old name of the PDSE member in the MEMBER field.

MONTH

Month the record was written. For SELECT/EXCLUDE processing, specify the first three characters of the month name (for example, JAN for January). The default output is also three characters long; specify an overriding output length of 9 characters to output the full month. This field is found in all SMF record types. For SELECT/EXCLUDE processing, a range of months separated by a colon (:) is allowed, as indicated in the following examples.

```
SELECT MONTH=JAN                        /* One month */
SELECT MONTH=(DEC, SEP)                 /* Two months */
SELECT MONTH>=MAY MONTH<=NOV            /* Month range */
SELECT MONTH=MAY:NOV                    /* Month range */
```

MONTHDAY, DAY

Day in month the record was written. This is a number in the range 1 to 31. This field is found in all SMF record types. For SELECT/EXCLUDE processing, a range of month days separated by a colon (:) is allowed, as indicated in the following examples.

```
SELECT MONTHDAY=15                      /* One day */
SELECT MONTHDAY=(15, 12)                /* Two days */
SELECT MONTHDAY>=2 MONTHDAY<=20         /* Day range */
SELECT MONTHDAY=2:20                    /* Day range */
```

MSGID

Message identifier. This field of at most 9 characters is only found in z/OS Firewall Technologies records (SMF record type 109).

NAME

Full user name or programmer name. It is found in:

- Job Initiation, Termination and Accounting records (SMF record types 5, 20, 30 and 32), where the name is taken from the job card.
- RACF processing records (SMF record types 80 and 83 subtype 1), where the name is taken from the ACEE,

OMCMD_ALLOWED

This is a flag field that indicates whether the command was suppressed by the security facility. (See 1336.

OMCMD_NAME

The OMCMD_NAME field contains the name of the Omegamon major or minor command that generated the audit record.

OMCMD_TYPE

The OMCMD_TYPE field indicates the Omegamon command type. Table 491 lists the possible types.

Table 491. Omegamon command types

Code	Description
I	Immediate
C	Major
M	Minor
G	Generalized Minor
S	Info line
P	Superceded command

For more information on the command types, see "*OMEGAMON® for MVS™ User's Guide* , SC27-2356-00 available at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.help.doc/welcome.htm.

OMCMD_TXT

The OMCMD_TEXT field contains the command text that was entered on the OMEGAMON II® screen. Records of minor commands also reference their associated major commands. This is the command string that caused the audit record to be generated, complete with parameters.

OWNER

RACF owner of the target profile (either a user id or a group id). This field is only found in RACF processing records (SMF record types 80 and 83 subtype 1).

To select the owner specified in a RACF command, use the RACFCMD_OWNER command field instead.

PKCS11_TOKEN

This field is found in RACF processing records (SMF record type 80) for the RACDCERT event, and corresponds with RACF_SECTION(399). It is present for the token manipulation subcommands of this event (`ADDTOKEN`, `BIND`, `DELTOKEN`, `IMPORT`, and `UNBIND`) and will contain the name of the token that was affected by the command.

PRIORITY

This field is only found in z/OS Firewall Technologies records (SMF record type 109). It indicates the priority of a record, which can range from Debug (lowest priority) to Emergency (highest priority). Its value can be Debug, Informational, Notice, Warning, Error, Critical, Alert, or Emergency.

PROCNAME

JCL procedure name. This field is only found in Accounting records (SMF record type 30).

PRODUCT

This value identifies the product from which the record was obtained. Table 492 lists the supported record types and value returned for each type.

Table 492. SMF NEWLIST PRODUCT field - possible values

Record type	Value returned
Customer Information Control System (CICS) performance monitoring records (SMF record type 110)	CICS
IBM Tivoli Key Lifecycle Manager audit records ((SMF record type 83, subtype 5)	TKLM-zOS
Websphere Application Server, version 7.0 audit records (SMF record type 83, subtype 5)	WAS-zOS

PRODUCT_FMID

This value identifies the FMID for the product that generated the SMF event record. The product name is returned in the PRODUCT field. This field is supported for the following record types:

- CICS monitoring records (SMF record type 110, subtype 1)
- Security audit event records from IBM Websphere Application Server, version 7.0 and later (SMF record type 83, subtype 5)
- Security audit event records from Tivoli Key Lifecycle Manager (SMF record 83, subtype 6)

PROFILE

RACF profile name. The type of the profile is rather dependent on the record type described. For common address space work records this field describes the userid that started the job. For data set and ICF catalog records, it will be the profile for the data set described in the record. For RACF records, it might be any type of profile. For RACF commands on a user or group, the profile describes the target user or group.

The PROFILE field is found in RACF processing and R_auditx records (SMF record types 80 and 83), and is derived for SMF record types 14, 15, 17, 18, 30, 42, 60, 62, 64, 65 and 66. To derive profile names for VSAM data set activity records (SMF record types 62 and 64), a CKFREEZE file with catalog information must be available for the system.

This is a repeated field, though most records contain only one profile.

The default output length of the PROFILE field is 44, which is sufficient for all profiles in class DATASET. General resource profiles might have a length of up to 255 characters.

Warning. Unlike the NEWLIST TYPE=RACF, using a generic value with the PROFILE field means that pattern match selection is used,
e.g. PROFILE=SYS1.** matches all profiles and resources that match the pattern SYS1.**. To select a specific generic resource, enclose the profile name in quotes, for example PROFILE='SYS1.**'.

PROGRAM

Program name. This field is only found in the following record types:

- Step Termination, Accounting
- ICF export (SMF record types 4, 30, 32, 34, and 36)
- DB2 SMF type 102 subtype/IFCid 22, 145, 177, and 183
- Security audit event records from IBM Websphere Application Server, version 7.0 and later (SMF record type 83, subtype 5) and Tivoli Key Lifecycle Manager (SMF record 83, subtype 6)

The default field length is 8, but the length can be up to 128 for DB2 SMF records. The default output format for this field shows the first 8 characters of the program name which can result in truncating file names. To include the full program name, use the following format specification in CARLa scripts: `program(0,wrap)`.

QUAL

RACF QUAL field. This field is equal to the HLQ of the data set, or the QUAL field of a naming convention table and/or exit. It defines the default owner of a data set. RACF will allow access without additional access checking.

This field is derived for RACF processing records (SMF record types 80 and 83 subtype 1), ICF catalog activity records and common address space work records (SMF record types 14, 15, 17, 18, 42, 60, 61, 62, 64, 65 and 66), and HSM function statistic records.

Note that when you have a naming convention table you must use a CKFREEZE for correct processing. When you have a naming convention exit you must run the program on the local system.

Note that RACF processing records will contain the resource names instead of the data set names when SETROPTS NOREALDSN is in effect. Consequently, it is not generally possible to deduce the correct QUAL from the record contents. In this case, the HLQ of the resource will be returned. If you have a naming convention table or exit that may change the QUAL to a value different from the HLQ of the resource name, this may occasionally be incorrect.

R_ACCESS

The `R_ACCESS` field is found in IBM Websphere Application Server, version 7.0 security audit records (SMF record type 83, subtype 5) and is set from relocate section 119 (`accPermGrant`) in the record.

R_ACTION

The `R_ACTION` field contains the action which caused the record to be created on the remote system. This field applies to IBM Tivoli Key Lifecycle Manager security audit records (SMF record type 83 subtype 6). The value is taken from the text following `action=` in relocate section 150 of the record. It also applies to security audit records from IBM Websphere Application Server, version 7.0 and later (SMF record type 83 subtype 6). In these records, the value is taken from relocate section 111 (`accAction`) of the record.

This field has a maximum length of 8.

R_EVENT

The `R_EVENT` field contains the event type that generated the log record. This field applies to audit security records associated with Tivoli Key Lifecycle Manager events (SMF record type 83, subtype 6) as indicated by the field PRODUCT. (See 1337.)

The `R_EVENT` field can also be found in the IBM Websphere Application Server, version 7.0 audit records.

Table 493 lists the event information that can be displayed.

Table 493. Event qualifier codes for SMF record types 83, subtype 6

TKLM Security Audit Event	Description	SMF Code	UNLOAD keyword <event type>
-- unknown --	Unknown events	1	*KLMUNKN
SECURITY_AUTHN	Authentication events	2	*KLMAUTN
SECURITY_AUTHN_TERMINATE	Authentication termination events	3	*KLMAUTT
SECURITY_AUTHZ	Authorization checks	4	*KLMAUTZ
SECURITY_DATA_SYNC	Data synchronization events	5	*KLMSYNC
SECURITY_MGMT_AUDIT	Management operations of the audit subsystem	6	*KLMAUDI
SECURITY_MGMT_CONFIG	Configuration operations for a security server	7	*KLMCONF
SECURITY_RUNTIME_KEY	Runtime operations for certificates/keystores	8	*KLMKEYR
SECURITY_MGMT_RESOURCE	Resource management	9	*KLMRESM
SECURITY_RUNTIME	Runtime starting and stopping of security servers.	10	*KLMRUNT

Table 494. Event qualifier codes for SMF record types 83, subtype 5

Audit Event from IBM Websphere Application Server, version 7.0 and later	SMF Event Qualifier	UNLOAD keyword <event type>
SUCCESS	0	SUCCESS
INFO	1	INFO
WARNING	2	WARNING
FAILURE	3	FAILURE
REDIRECT	4	REDIRECT
DENIED	5	DENIED
ERROR	6	ERROR

R_INTENT

The R_INTENT field specifies the type of access requested when this event record was logged. This field applies to IBM Websphere Application Server, version 7.0 security audit records (SMF record type 83 subtype 5). In these records, the value is taken from relocate section 118 (`accPermCheck`) of the record.

R_LOGDATA

This repeated field returns information about a security audit event from a zLinux system (SMF record type 83, subtype 4 event records). The information is provided in a `fieldname=value` format with a separate entry for each value returned. The values are found in the relocate 114 field of the SMF record and depend on the type of event that was logged.

SMF record type 83, subtype 4 event records are only created for zLinux systems that have been set up for remote monitoring using either the *audispd* plugin or the JZOS toolkit. For additional information about these records and setting up remote auditing, see the *Enterprise Multiplatform Auditing, IBM Redbook* available at http://www.redbooks.ibm.com/abstracts/sg247472.html.

Also see, the 1344 and 1344RACF_LINK_EVENT fields.

R_LOGRECORD

The R_LOGRECORD fields contains the native Java log record for use by IBM Tivoli Compliance Insight Manager Enabler for z/OS. This field applies to security audit records (SMF type 83 subtype 6 event records). This field has a maximum length of 1024.

R_MGMT_ATTR

The R_MGMT_ATTR provides information about one or more secondary objects involved in the operation that generated this record. This field can be found in security audit records from IBM Websphere Application Server, version 7.0 and later (SMF record type 83, subtype 5). The value is taken from relocate section 155 (mgmtAttr) of the record.

R_MGMT_CMD

The R_MGMT_CMD field identifies the application-specific command that was being performed during the event that generated this record. This field can be found in security audit event records from IBM Websphere Application Server, version 7.0 or later (SMF record type 83, subtype 5). The value is taken from relocate section 154 (mgmtCmd).

R_MGMT_TYPE

The R_MGMT_TYPE field indicates the type of management operation that was being performed during the event that generated this record. This field can be found in security audit event records from IBM Websphere Application Sever, version 7.0 or later (SMF record type 83, subtype 5). The value is taken from relocate section 153 (mgmtType) of the record.

R_RESOURCE

The R_RESOURCE field contains the name of the resource in the context of the application that generated the event record. This field applies to IBM Tivoli Key Lifecycle Manager audit records (SMF record type 83, subtype 5). The value is taken from relocate section 150 (resource=[name=) of the record.

This field can also be found in security audit event records from IBM Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5). In these records, the value is taken from relocate section 114 (accApplName) of the record.

This field has a maximum length of 64. The actual length might be longer than the default length.

R_RESULT

The R_RESULT field This field is found in security audit event records from IBM Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5). The value is taken from relocate section 114 (accDecision) of the record.

R_ROLECHECK

The R_ROLECHECK field indicates the roles that were checked when the event record was generated. This field is found in security audit records from IBM

Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5). The value is taken from relocate section 120 (accRoleCheck) of the record.

R_ROLEGRANT

The R_ROLEGRANT field indicates the roles that were granted when the event record was generated. This field is found in security audit records from IBM Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5). The value is taken from relocate section 121 (accRoleGrant)) of the record.

R_USER

The R_USER field contains the userid used by the product or component for purposes of the authentication or authorization request that generated this record. This field is found in Tivoli Key Lifecycle Manager audit records (SMF record type 83, subtype 6). The value is taken from the relocate section 150 (user=[name=) of the record.

This field also applies to security audit records from IBM Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5). In these records, the value is taken from relocate section 113 (accApplUser) of the record.

RACFAUTH, AUTHORITY

RACF authority used. This field is only found RACF processing and R_auditx records (SMF record type 80 and 83). It is used to select records by the RACF authority used for executing commands or accessing resources, e.g. SPECIAL or OPERATIONS. When used for output, the default output is condensed; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 10, for example RACFAUTH(EXPLODE,10). The table [13] Table 495 shows the RACFAUTH values and their meanings.

Table 495. SMF RACFAUTH and AUTHORITY fields - values for output processing

SELECT/EXCLUDE value	Output code	Exploded output	Meaning
AUDITOR	A	Auditor	AUDITOR attribute
BYPASS BYPASSED	B	Bypass	Bypassed-user id = *BYPASS*
EXIT	X	Exit	Installation exit processing
FAILSOFT	F	Failsoft	Failsoft processing
NORMAL	N	Normal	Normal authority check
OPERATIONS	O	Operations	OPERATIONS attribute
SPECIAL	S	Special	SPECIAL attribute
SUPER SUPERUSER	Su	Superuser	OpenEdition MVS super-user (uid 0)
SYSTEM	**Sy**	System	OpenEdition MVS system function
TRUSTED	T	Trusted	Trusted/Privileged attribute

13. Bypass appears for actions on operator consoles where no operator is logged on (and is not required to logon), and success auditing has been requested for OPERCMDS profiles.

Note: For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

RACFCMD

RACF logged command. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for events dealing with RACF commands. To find all records with a RACFCMD field, select either EXISTS(RACFCMD) or EVENT=ALLCOMMAND.

To select specific RACF commands you can do a field compare on the RACFCMD field or use the EVENT field. To select the target profile (data set, general resource, user, or group), use the PROFILE field. To select the target user of a command, use the RACFCMD_USER field. To select the target group of a command, use the RACFCMD_GROUP field. To select RACF commands where specific keywords or options were used, use the RACFCMD_KEYWORDS field.

The RACFCMD field is a repeated field; the first entry prints the RACF command name; each following entry prints a logged command parameter, appended by <**Ignored**> for parameters ignored because of insufficient authority, and <**Error**> for parameters ignored because of a processing error. Passwords, which are not logged in SMF records, are indicated by the string <**Password**>.

The default output length of the RACFCMD field is 64 characters; the full length may be up to 32000 characters for SETROPTS commands. To print the command in one string, use the output modifier HORIZONTAL, e.g. RACFCMD(HORIZONTAL). To print long commands in a column, use the output modifiers HORIZONTAL and WRAP, e.g. RACFCMD(WRAP,HORIZONTAL,60).

Note: The RACFCMD field cannot be used for forward recovery (by reissuing the RACF commands), because the command result depends on the issuer, and with forwarded recovery the issuer is generally someone else. RACF does log some implied default parameters, but not all implied parameters (e.g. the current user as owner). The RACFCMD field may therefore not correspond exactly to the command typed, but it will be equivalent.

RACFCMD_AUTH

The (new) group authority specified in a RACF logged command. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for events dealing with RACF commands.

The RACFCMD_AUTH field is defined for ADDUSER, ALTUSER, and CONNECT commands. Possible RACFCMD_AUTH values are documented in the following table (increasing sort order).

Table 496. SMF record RACFCMD_AUTH field - possible values and descriptions

RACFCMD_AUTH value
USE
CREATE
CONNECT
JOIN

RACFCMD_EFFECTIVE

RACF logged command, without ignored and erroneous keywords and values. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for events dealing with RACF commands. It can be used for output and SELECT/EXCLUDE processing.

The RACFCMD_EFFECTIVE field is a repeated field; the first entry prints the RACF command name; each following entry prints a logged command parameter. Parameters ignored because of insufficient authority, and parameters ignored because of a processing error is not shown. Passwords, which are not logged in SMF records, are indicated by the string <Password>.

RACFCMD_GROUP

The target group of a RACF logged command. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for the ADDUSER, ALTUSER, ADDGROUP, ALTGROUP, CONNECT, DELGROUP, REMOVE, and PERMIT commands.

For ADDGROUP, ALTGROUP and DELGROUP this field reports the group that is defined or altered; it is equal to the RESOURCE and PROFILE fields.

For ADDUSER, ALTUSER, CONNECT and REMOVE, this field reports the group that is used to define, alter or remove a connect. The value corresponds to the value of the DFLTGRP keyword for ADDUSER and the GROUP keyword for ALTUSER, CONNECT and REMOVE. (The RESOURCE and PROFILE fields describe the target user.)

For PERMIT this field reports all PERMIT ids known to be groups. Note that this requires access to a RACF database or unload, with the group present in the DB, because the SMF records contain the IDs specified on the PERMIT commands, without the indication whether they are users or groups.

RACFCMD_KEYWORDS

The repeated field contains the keywords used with a logged RACF command.

This field contains one repeat-group entry for each keyword used in a RACF command. The RACF command itself, and the *values* used with the keywords, are not included. So, for the command CONNECT XX GROUP(YY) NOSPECIAL AUTHORITY(USE), the RACFCMD field would contain the values GROUP, NOSPECIAL, and AUTHORITY.

The main use of this field is to select or exclude commands that use specific keywords that are allowed or disallowed. For instance, to select all CONNECT commands that use any parameter other than GROUP, use SELECT EVENT=CONNECT RACFCMD_KEYWORDS<>GROUP. A list of keywords, as well as substrings and generic values, may be specified as with any other character field.

RACFCMD_KEYWORDS_EFF

The repeated field contains the effective (not erroneous or ignored) keywords used with a logged RACF command. It can be used for output and SELECT/EXCLUDE processing.

This field contains one repeat-group entry for each keyword used in a RACF command. The RACF command itself, and the values used with the keywords, are not included. So, for the command CONNECT XX GROUP(YY) SPECIAL AUTHORITY(USE), the RACFCMD_KEYWORDS_EFF field would contain the values GROUP, SPECIAL, and AUTHORITY. If the issuing user did not have authority to issue the SPECIAL keyword for this connect, the field would only contain the values GROUP and AUTHORITY.

The main use of this field is to select or exclude commands that use specific keywords that are allowed or disallowed. For instance, to select all CONNECT commands that use any parameter (that actually got executed) other than GROUP, use SELECT EVENT=CONNECT RACFCMD_KEYWORDS_EFF<>GROUP. A list of keywords, as well as substrings and generic values, may be specified as with any other character field.

RACFCMD_OWNER

The (new) owner specified in a RACF logged command. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for events dealing with RACF commands.

The RACFCMD_OWNER field is defined for ADDGROUP, ADDSD, ADDUSER, ALTDSD, ALTGROUP, ALTUSER, CONNECT, RALTER, RDEFINE, and REMOVE commands.

RACFCMD_USER

The target user of a RACF logged command. This field is found in RACF processing records (SMF record types 80 and 83 subtype 1) for events dealing with RACF commands.

The RACFCMD_USER field is defined for ADDUSER, ALTUSER, CONNECT, DELUSER, PASSWORD, REMOVE, RACDCERT, RACLINK and PERMIT commands.

For all events except PERMIT RACDCERT and RACLINK, it is equal to the RESOURCE and PROFILE fields.

For the PERMIT command, it reports all PERMIT ids known to be users. Note that this requires access to a RACF database or unload, with the user present in the DB, because the SMF records contain the IDs specified on the PERMIT commands, without the indication whether they are users or groups.

For the RACLINK commands the target user is reported.

For RACDCERT the userid associated with the certificate is reported.

RACF_LINK_AUDIT

Returns a link value for connecting security audit event records related to the same event. This value applies to RACF processing and remote audit event records (SMF record type 80 and SMF record type 83). Records that have the same value for the RACF_LINK_AUDIT and RACF_LINK_EVENT fields are connected to the same event.

See also 1344.

RACF_LINK_EVENT

Returns the event serial number for a security audit event from a zLinux system. This field applies to SMF record type 83, subtype 4 event records created through remote monitoring of a Linux system. Records with the same RACF_LINK_EVENT value are associated with the same event. Application-specific information about the security audit event is returned in the R_LOGDATA field.

You can use the RACF_LINK_EVENT value in combination with the RACF_LINK_AUDIT value for identifying the RACF command processing that caused the security audit event to be logged. Records that have the same RACF_LINK_EVENT and RACF_LINK_AUDIT values are associated with the same event.

SMF record type 83, subtype 4 event records are only created for zLinux systems that have been set up for remote monitoring using either the *audispd* plug-in or the JZOS toolkit. For additional information about these records and setting up remote auditing, see the *Enterprise Multiplatform Auditing, IBM Redbook* available at http://www.redbooks.ibm.com/abstracts/sg247472.html.

RACF_SECTION

This pseudo-field can be used to create user-defined SMF fields, to select and display values not provided for by the existing, built-in fields. It can be used for values described by a RACF relocate section within the SMF record. For a full description and examples of use, see "Defining fields in SMF records" on page 767.

REASON

RACF reason for logging. This field is only found RACF processing and R_auditx records (SMF record type 80 and 83). This field is used to select records by the RACF reason for logging, for example, SPECIAL users being audited or logging due to SETROPTS LOGOPTIONS.When used for output, the default output is condensed; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 15, for example, REASON(EXPLODE,15).

The REASON field shows the information that RACF logged. When no REASON value has been specified by the issuer of the log record, the value is shown as blanks. You may select or exclude such records by using the value NONE. This value cannot be combined with other values in a list specification.

The following table shows the REASON values and their meanings.

Table 497. SMF record REASON field - values for output processing

SELECT/EXCLUDE	Output code	Exploded output	Meaning
ACCESS RESOURCE	Ac	Resource	Access to the resource is being audited due to the AUDIT option, a logging request from the RACHECK exit routine, or because the operator granted access during failsoft processing
APPLAUDIT	Ap	Applaudit	Entity audited due to SETROPTS APPLAUDIT
CLASS	Cl	Class	SETROPTS AUDIT(class) - Changes to this class of profile are being audited
CMDVIOL	Vi	CmdViol	Violation detected in command and CMDVIOL is in effect
COMMAND ALWAYS	Cm	Command	RVARY or SETROPTS command issued: these commands are always audited
COMPATMODE COMPAT	Co	Compatmode	Entity audited due to SETROPTS COMPATMODE
GLOBALAUDIT GLOBAL AUDITOR	G	Global audit	Access to entity being audited due to GLOBALAUDIT option
LOGOPTIONS	O	Logoptions	Class being audited due to SETROPTS LOGOPTIONS
NONE	blank	blank	No REASON value present in SMF record.
OMVS_AUTHORITY	Oa	OMVS authority	Audited because user does not have appropriate authority in OpenEdition MVS
OMVS_UNDEFINED	Ou	OMVS undefined	Audited because user not defined to OpenEdition MVS

Table 497. SMF record REASON field - values for output processing (continued)

SELECT/EXCLUDE	Output code	Exploded output	Meaning
RACINIT	R	Racinit failure	RACINIT failure
SECLABELAUDIT SECLABEL	Sl	Seclabel	Entity audited due to SETROPTS SECLABELAUDIT
SECLEVEL SECAUDIT	L	Seclevel	Entity audited due to SETROPTS SECLEVELAUDIT
SPECIAL	Sp	Special	SPECIAL or OPERATIONS users being audited (due to SETROPTS SAUDIT or SETROPTS OPERAUDIT).
USER	U	User	User being audited (due to ALTUSER UAUDIT)
VMEVENT VMAUDIT	Vm	VM event	VMEVENT auditing

Note: For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

RECNO

Record number of the current record within its input file (not overall). The RECNO field applies to the number of complete **logical** records within a single input file, counting the first record as 1. Found in all record types. Note: For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

RECORD

The RECORD field contains a single full record. It is designed to be used with a `DUMP` format, or in the DEFINE command. For information, see "DEFINE" on page 750, in combination with field-value manipulation functions in "Field value manipulation" on page 760.

Note: This field has format ASIS by default, which has been built specifically to keep trailing spaces and nulls intact. This format is also inherited by fields defined with RECORD as base. When trailing spaces should be trimmed, the overriding format CHAR can be used.

RECORDDESC

A descriptive string summarizing the record. This field is found in all predefined record types and is for output only. For most record types, a stock description is printed; for some record types, notably Accounting, Data set and Catalog activity, RACF/ACF2/TSS processing, and HSM function statistics, the description prints a string summarizing the record, often including the userid or data set name. The default length of the field is 150. The maximum length is 32760.

Notes:

1. The values printed by the RECORDDESC field are subject to change. Do not write applications that are dependent on the output of this field.
2. For path names to appear in the RECORDDESC fields of OpenMVS File System activity records (SMF record type 92) with subtypes 10 (open file) and 11 (close file), a CKFREEZE needs to be present in the input files of your setup.

RECORDLENGTH, RECORD_LENGTH

This field describes the length of the SMF record in bytes, including the SMF record header and the RDW. The given length is the one of the **logical** record. It is a decimal number of up to 32767. This field is available in all record types.

RELOCATE

This field is meant for debugging purposes. It is only found in RACF processing and R_auditx records (SMF record types 80 and 83). It can be used to select records containing specific relocate section codes; when used for output, all relocate sections contained in the record are printed. This is a repeated field, with one entry for each relocate section type found.

Older RACF relocate section codes are in the range 0 to 255; relocate section codes produced by OMVS auditing and Certificate processing are in the range 256 and upwards.

Note: For SELECT/EXCLUDE processing, only the = relational operator can be used.

RESOURCE

SAF resource name. This field is found in the following record types:

- RACF processing and R_auditx records (SMF record types 80 and 83)
- TSS processing records (SMF record type 80)

This field is derived for data set, ICF catalog activity records, and common address space work records (SMF record types 14, 15, 17, 18, 30, 42, 60, 62, 64, 65 and 66). To derive resource names for VSAM data set activity records (SMF record types 62 and 64), a `CKFREEZE` file with catalog information must be available for the system.

This is a repeated field. However, most records contain only one resource.

The default output length of the `RESOURCE` field is 44, which is sufficient for all resource names in the `DATASET` class. General resource names can have a length of up to 255 characters.

RTOKEN

An *output only* field that contains a string describing the contents of the Resource Security Token included in some RACF processing records (SMF record types 80 and 83 subtype 1) with EVENT=ACCESS. Because the `RTOKEN` value contains many fields–many that need not be set, the output has the format `field1: value1; field2: value2`.

To select all records with an `RTOKEN` field, use `SELECT RELOCATE=54`. To select on values contained in the `RTOKEN` field, use the derived field `RTOKEN_FLAGS`.

Note: The values printed by the `RTOKEN` field are subject to change. Do not write applications that are dependent on the output of this field.

RTOKEN_FLAGS

Describes the flags found in the Resource Security Token, which is included in some RACF processing records (SMF record types 80 and 83 subtype 1) with EVENT=ACCESS. It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the RTOKEN field is more convenient for output. See the UTOKEN_FLAGS field for a description of the values in this field.

Note: The values printed by the RTOKEN_FLAGS field are subject to change. Do not write applications that are dependent on the output of this field.

SECLABEL

The security label for the user. This field is found in the following record types:

- RACF processing and R_auditx records (SMF record types 80 and 83) if your installation has activated the SECLABEL class through a SETROPTS CLASSACT(SECLABEL) command.
- DB2 records (SMF record type 102) with subtypes/IFCids 83, 87, 140, 142, 269, and 314 if non-blank and non-null.
- CSSMTP client records (SMF record type 119) with subtype 48 if non-blank and non-null.

SECURITY_EVENT

Identifies a high-level security event. Currently, zSecure Admin and Audit only support this field for the following record types:

- DB2 audit records (SMF record type 102) with subtype/IFCid 4, 5, 6, 7, 8, 9, 10, 22, 23, 24, 25, 33, 34, 35, 36, 37, 38, 39, 40, 41, 55, 63, 83, 87, 90, 91, 92, 97, 104, 106, 107, 114, 115, 116, 118, 119, 120, 140, 141, 142, 143, 144, 145, 169, 177, 219, 220, 258, 269, 270, 271, 314, 319, 350, 361, 362 if non-blank and non-null.
- z/OS UNIX File System Activity, security attribute audit records (SMF record type 92, subtype 15).

Note: The values printed by the SECURITY_EVENT field are subject to change. Do not write applications that are dependent on the default output of this field. You can use the overriding output format `dec` to use this field as a programming interface.

Table 498. SMF record SECURITY_EVENT field - output formats

Default output format	"dec" format	Explanation
Logon user success	1	Successful user logon
Logon user warning	2	Warning user logon
Logon user failure	3	Failed user logon
Logoff user	4	User logoff
Session start success	5	Successful batch/started task start
Session start warning	6	Warning batch/started task start
Session start failure	7	Failed batch/started task start
Session end	8	Batch/started task end
Access success	9	Successful access attempt
Access warning	10	Warning access attempt
Access failure	11	Failed access attempt

SIG_DATE

Text field that specifies the date that the module was signed.

SIG_ENTITY_DN

Text field that provides the program signer (End Entity) certificate subject's distinguished name.

SIG_EXPIRATION

Text field that specifies the date when the module certificate chain expires.

SIG_PROGRAM_LOADED

Flag field that indicates whether the Signature Verification program was loaded for this event record.

SIG_ROOT_DN

Text field contains the distinguished name for the root signing certificate subject's distinguished name.

SIG_TIME

Text field that specifies the time that the module was signed.

SMFDD

Contains the ddname of the Security zSecure SMF input file. The value can be *SMF* or in the range *SMF00-SMF99*. Supported for all SMF record types.

SMFUSERID, SMFUSER

User identification field from the SMF common exit parameter area. This field is found in most process-related record types. If your installation has an exit that writes a user ID in the common exit area, the value represents the user ID. Otherwise, the value is *0*.

SMF_FIELD

This pseudo-field can be used to create user-defined SMF fields, to select and display values not provided for by the existing, built-in fields. It can be used for values at a constant offset within the SMF record. For a full description and examples of use, see "Defining fields in SMF records" on page 767.

SMF_SECTION

This pseudo-field can be used to create user-defined SMF fields, to select and display values not provided for by the existing, built-in fields. It can be used for values described by a so-called self-defining section within the SMF record. For a full description and examples of use, see "Defining fields in SMF records" on page 767.

SPECIALTYPE

This field is an identifier for records that cannot be uniquely recognized from their numerical TYPE alone, either because the SMF record number for a specific application is not static (field values `ACF2`, `HSM0`, `HSM1`, `AIM`, `OMEG`, and `SECURPASS`) or because an application reuses a number that is officially assigned to another application (field value TSS). The SMF record numbers that correspond to each SPECIALTYPE is determined from the CKFREEZE file for a system, or from `SIMULATE SMF` commands. (See "SIMULATE" on page 911.)

SRCHOST

The `SRCHOST` field contains the port number of the remote host for this event record. This field is found in security audit records from IBM Websphere Application Server, version 7.0 or later (SMF record 83, subtype 5) and in NFS audit statistics records (SMF record type 42 subtype 26). The value is taken from relocate section 108 (`sessRemHost`) of the record.

SRCIP

Source IP address. This field is found in the following record types:

- z/OS Firewall Technologies records

- SMF record type 109, SMF record type 118 (IPv4)
- SMF record type 119 (IPv6)
- SMF record type 102 subtype/IFCid 269 and 319
- SMF record type 110 subtype 1 (CICS performance monitoring record)
- SMF record type 83 subtype 5 (audit records from IBM Websphere Application Server, version 7.0 or later)
- SMF record type 42 subtype 26 (NFS audit statistics)

For Websphere Application Server audit records, the value is taken from relocate section 106 (`sessRemAddr`) of the record.

SRCPORT

Source port number. This field is found in the following record types:

- z/OS Firewall Technologies records
- SMF record type 109
- SMF record type 118 (IPv4)
- SMF record type 119 (IPv6)
- SMF record type 83 subtype 5 (audit records from IBM Websphere Application Server, version 7.0 or later)

For Websphere Application Server audit records, the value is taken from relocate section 107 (`sessRemPort`) of the record.

STEPNAME

Step name. This field is found in the following record types:

- Step Termination and Accounting records (SMF record types 4, 30, 32, 33, and 34).
- z/OS UNIX File System Activity, security attribute audit records (SMF record type 92, subtype 15).
- ACF2 data set use records.

SUBSYS

This field contains the 4 character subsystem name. The SMF standard header has an architected place for a subsystem name under the control of a bit in the SMF header. If one is present, it is returned, unless it is always empty (type 41) or the flag is on by accident (type 118). In addition, some record types report a subsystem name even though the header flag says not. This applies to type 59, 99, 100, 101, and 102.

SUBSYS_TYPE

This field describes the subsystem type that generated the SMF record. It is only filled in if a CKFREEZE file is used. Currently this field only recognizes JES2 and JES3 subsystems. For other subsystems, or SMF records not created by a subsystem, it is missing. You can select on this field by using its byte-value. Table 499 shows the possible values:

Table 499. SMF record SUBSYS_TYPE field values

Subsys value	Description
X'02'	JES2
X'03'	JES3

SUBRECORD

CICS SMF 110 Monitoring performance records contain many Performance Data sections, relating to separate CICS events. These repeated sections are processed as if they are single ordinary SMF records. This field contains the full Performance subrecord. The complete SMF record can be found in the RECORD field.

SUBRECORDNO

This field returns the value of the current subrecord number within the full SMF record. This field is only supported in CICS monitoring performance records (`CICS_MONITOR_CLASS = 3`). See 1350.

SUBTYPE

This field contains the SMF record subtype and can only be used for output; for SELECT/EXCLUDE processing, it is selected implicitly with the TYPE field, see Table 500 on page 1352. This field is found in all records that have subtypes, for example SMF record types 24, 30, 32, 33, 41, 42, 83 and 110. The SMF record header is examined to determine whether subtypes are present; as a result, subtypes are also found in record types for which only basic support is available.

The following tables show supported subtype values and their meaning:

- Table 500 on page 1352 *SMF record type 24: JES2 Spool Offload SUBTYPEs*
- Table 501 on page 1352 *SMF record type 30: Common Address Space Work SUBTYPEs*
- Table 502 on page 1352 *SMF record type 32: TSO/E User Work Accounting SUBTYPEs*
- Table 503 on page 1352 *SMF record type 33: APPC/MVS TP Accounting SUBTYPEs*
- Table 504 on page 1353 *SMF record type 41: DIV ACCESS/UNACCESS SUBTYPEs*
- Table 505 on page 1353 *SMF record type 42: DFSMS Statistics and Configuration*
- Table 506 on page 1353 *SMF record type 70: RMF CPU Activity SUBTYPEs*
- Table 507 on page 1353 *SMF record type 72: RMF Workload Activity and Storage Data SUBTYPEs*
- Table 508 on page 1353 *SMF record type 74: RMF Device and XCF Activity SUBTYPEs*
- Table 509 on page 1353 *SMF record type 78: RMF Monitor I Activity SUBTYPEs*
- Table 510 on page 1354 *SMF record type 79: RMF Monitor II Activity*
- Table 511 on page 1354 *SMF record type 82: ICSF Integrated Cryptographic Facility SUBTYPEs*
- Table 512 on page 1355 *SMF record type 83: Security events SUBTYPEs*
- Table 513 on page 1355 *SMF record type 85: OAM Object Access Method SUBTYPEs*
- Table 514 on page 1356 *SMF record type 88: System Logger Data SUBTYPEs*
- Table 515 on page 1356 *SMF record type 89: Product Usage Data SUBTYPEs*
- Table 516 on page 1356 *SMF record type 90: System Status SUBTYPEs*
- Table 517 on page 1357 *SMF record type 91: Batch Pipes/MVS Statistics SUBTYPEs*
- Table 518 on page 1357 *SMF record type 92: OpenMVS File System Activity SUBTYPEs*

- Table 519 on page 1357 *SMF record type 94: IBM Tape Library Dataserver Statistics SUBTYPEs*
- Table 520 on page 1358 *SMF record type 96: The Integrated Reasoning System TIRS statistics SUBTYPEs*
- Table 521 on page 1358 *SMF record type 99: System Resource Manager decision SUBTYPEs*
- Table 522 on page 1358 *SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs*
- Table 523 on page 1370 *SMF record type 103: IBM HTTP Server SUBTYPEs*
- Table 524 on page 1370 *SMF record type 110: CICS Records SUBTYPEs*
- Table 525 on page 1371*SMF record type 115: MQSeries Statistics SUBTYPEs*
- Table 526 on page 1371 *SMF record type 119: Connectivity Statistics SUBTYPEs*
- Table 527 on page 1372 *SMF record type 120: Websphere AS Performance Statistics SUBTYPEs*

Table 500. SMF record type 24: JES2 Spool Offload SUBTYPEs

Subtype	Meaning
1	Job Transmitted
2	Job Received
3	SYSOUT Transmitted
4	SYSOUT Received

Table 501. SMF record type 30: Common Address Space Work SUBTYPEs

Subtype	Meaning
1	Job start
2	Interval
3	Step termination
4	Step total
5	Job termination
6	System address space

Table 502. SMF record type 32: TSO/E User Work Accounting SUBTYPEs

Subtype	Meaning
1	TSO/E User Interval
2	TSO/E User Session End
3	TSO/E User Detail Interval Record
4	TSO/E User Detail Session End

Table 503. SMF record type 33: APPC/MVS TP Accounting SUBTYPEs

Subtype	Meaning
1	APPC/MVS Transaction
2	APPC/MVS Conversation

Table 504. SMF record type 41: DIV ACCESS/UNACCESS SUBTYPEs

Subtype	Meaning
1	DIV ACCESS
2	DIV UNACCESS
3	VLF Statistics

Table 505. SMF record type 42: DFSMS Statistics and Configuration SUBTYPEs

Subtype	Meaning
20	STOW Initialize
21	Member Delete
22	DFSMSrmm Audit Records Section
23	DFSMSrmm Security Section
24	Member Add/Replace
25	Member Rename
26	NFS Create/Delete/Rename statistics

Table 506. SMF record type 70: RMF CPU Activity SUBTYPEs

Subtype	Meaning
1	RMF CPU, PR/SM™, and ICF Activity
2	RMF Cryptographic Hardware Activity

Table 507. SMF record type 72: RMF Workload Activity and Storage Data SUBTYPEs

Subtype	Meaning
1	RMF Workload Activity (compatibility mode)
2	RMF Storage data (compatibility mode)
3	RMF Workload Activity (goal mode)
4	RMF Storage data (goal mode)
5	RMF System suspend lock and GRS data

Table 508. SMF record type 74: RMF Device and XCF Activity SUBTYPEs

Subtype	Meaning
1	RMF Device Activity
2	RMF XCF Activity
3	RMF OMVS Facility Activity
4	RMF Coupling Facility Activity
5	RMF Cache Subsystem Activity
6	RMF HFS Statistics
7	RMF FICON® Director Statistics

Table 509. SMF record type 78: RMF Monitor I Activity SUBTYPEs

Subtype	Meaning
1	RMF I/O Queuing Activity (4381)
2	RMF Virtual Storage Activity

Table 509. SMF record type 78: RMF Monitor I Activity SUBTYPEs (continued)

Subtype	Meaning
3	RMF I/O Queuing Activity

Table 510. SMF record type 79: RMF Monitor II Activity

Subtype	Meaning
1	RMF Address Space State Data
2	RMF Address Space Resource Data
3	RMF Storage/Processor Data
4	RMF Paging Activity
5	RMF Address Space SRM Data
6	RMF Reserve Data
7	RMF Enqueue Contention Data
8	RMF Transaction Activity
9	RMF Device Activity
10	RMF Domain Activity
11	RMF Page Data Set Activity
12	RMF Channel Path Activity
13	RMF I/O Queuing Activity (4381)
14	RMF I/O Queuing Activity
15	RMF IRLM Long Lock Detection

Table 511. SMF record type 82: ICSF Integrated Cryptographic Facility SUBTYPEs

Subtype	Meaning
1	ICSF start
3	ICSF crypto processor added/removed
4	ICSF crypto failure or tampering
5	ICSF change to special security mode
6	ICSF key part entered through KEU
7	ICSF key part entered through KEU
8	ICSF in-storage CKDS copy refreshed
9	ICSF CKDS dynamically updated
10	ICSF PKA master key part entered
11	ICSF clear master key part entered
12	ICSF key loaded from TKE workstation
13	ICSF CKDS dynamically updated
14	ICSF PCI Cryptographic Coprocessor clear master key entry
15	ICSF PCI Cryptographic Coprocessor retained key create/delete
16	ICSF PCI Cryptographic Coprocessor TKE
17	ICSF PCI Cryptographic Coprocessor timing
18	ICSF PCI Cryptographic Coprocessor configuration
19	ICSF PCI X Cryptographic Coprocessor timing

Table 512. SMF record type 83: Security events SUBTYPEs

Subtype	Meaning
1	RACF Processing Record for Auditing Data Sets: Security Label Change
2	EIM Processing
3	LDAP audit data
4	R_auditx remote auditing service
5	IBM Websphere Application Server audit data
6	Tivoli Key Lifecycle Manager audit data

Table 513. SMF record type 85: OAM Object Access Method SUBTYPEs

Subtype	Meaning
1	OAM OSREQ Access
2	OAM OSREQ Store
3	OAM OSREQ Retrieve
4	OAM OSREQ Query
5	OAM OSREQ Change
6	OAM OSREQ Delete
7	OAM OSREQ Unaccess
32	OAM Storage Group Processing
33	OAM DASD space management
34	OAM Optical Disk Recovery Utility
35	OAM MOVEVOL Utility
36	OAM Single Object Recovery Utility
37	OAM OSMC Space Management
64	OAM LCS Optical Drive Vary Online
65	OAM LCS Optical Drive Vary Offline
66	OAM LCS Optical Library Vary Online
67	OAM LCS Optical Library Vary Offline
68	OAM LCS Optical Cartridge Eject
69	OAM LCS Optical Cartridge Entry
70	OAM LCS Optical Cartridge Label
71	OAM LCS Optical Volume Audit
72	OAM LCS Optical Volume Mount
73	OAM LCS Optical Volume Demount
74	OAM LCS Optical Write request
75	OAM LCS Optical Read request
76	OAM LCS Optical Logical Delete Request
77	OAM LCS Optical Physical Delete Request
78	OAM LCS Object Tape Write Request
79	OAM LCS Object Tape Read Request
87	OAM LCS Object Tape Volume Demount
88	OAM LCS Object Tape Logical Delete

Table 513. SMF record type 85: OAM Object Access Method SUBTYPEs (continued)

Subtype	Meaning
90	OAM LCS File System Write Request
91	OAM LCS File System Read Request
92	OAM LCS File System Physical Delete
93	OAM LCS File System Delete-Store Cleanup

Table 514. SMF record type 88: System Logger Data SUBTYPEs

Subtype	Meaning
1	System log: Stream Activity
11	System log: CF Alter Activity

Table 515. SMF record type 89: Product Usage Data SUBTYPEs

Subtype	Meaning
1	Product Usage Data
2	Product State Data

Table 516. SMF record type 90: System Status SUBTYPEs

Subtype	Meaning
1	SET TIME
2	SET DATE
3	SET DMN
4	SET IPS
5	SET SMF
6	SWITCH SMF
7	HALT EOD
8	IPL PROMPT
9	IPL SMF
10	IPL SRM
11	SET OPT
12	SET ICS
13	SET SMF
14	SET MPF
15	RESTART SMF
16	SET DAE
17	SET PFK
18	SET GRSNRL
19	SET APPC
20	SET SCHPRM
21	SET SCH
22	SET CNGRP
23	WLM Service Definition Install

Table 516. SMF record type 90: System Status SUBTYPEs (continued)

Subtype	Meaning
24	WLM Service Policy Activation
25	Workload Management Mode Change
26	IPL LOGREC
27	ARM restarts enabled
28	ARM restarts disabled
29	SET PROG (LNKLST set activation)
30	RESET command completed
31	SET PROG (LPA Set Activation)
32	Scheduling Environment Information

Table 517. SMF record type 91: Batch Pipes/MVS Statistics

Subtype	Meaning
1	Batch pipe Subsystem Start
2	Batch pipe Subsystem Interval Expiration
3	Batch pipe Subsystem Stop
11	Batch pipe Open-Connection
12	Batch pipe Interval Expiration
13	Batch pipe Close-Connection
14	Batch pipe Creation
15	Batch pipe Deletion

Table 518. SMF record type 92: OpenMVS File System Activity SUBTYPEs

Subtype	Meaning
1	UNIX File System mounted
2	UNIX File System suspended
4	UNIX File System resumed
5	UNIX File System unmounted
6	UNIX File System remounted
7	UNIX File System moved
10	UNIX file opened
11	UNIX file closed
12	UNIX mmap service
13	UNIX munmap service
15	UNIX security attributes (APF authorization, program control, or shared library) changed.

Table 519. SMF record type 94: IBM Tape Library Dataserver Statistics SUBTYPEs

Subtype	Meaning
1	34xx Library Statistics

Table 520. SMF record type 96: The Integrated Reasoning System TIRS statistics SUBTYPEs

Subtype	Meaning
1	The Integrated Reasoning System detail statistics
2	The Integrated Reasoning System summary statistics

Table 521. SMF record type 99: System Resource Manager decision SUBTYPEs

Subtype	Meaning
1	SRM system level data
2	SRM service class data
3	SRM service class period plot data
4	SRM device cluster data
5	SRM monitored address space data
6	SRM next interval resource settings
7	SRM PAV device data
8	SRM WLM LPAR partition data
9	SRM IOS subsystem data

The subtypes for SMF record types 100, 101, and 102: DB2 Performance and Audit represent the IFCid. Its meaning can be printed with format `DB2_IFCid`. Table 522 shows the subtypes, whether they use or define numeric Data Base Ids, Object Ids, or Data Set Ids (`DBIDs`, `OBIDs`, and `DSIDs`), and what fields are filled in with detailed information from the subtype relocate sections.

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs

Subtype	Meaning	Specific field support	Trace class or IFCID
0	Normal trace record		GLOB(3)
1	System statistics		STAT(1), MON(1), PERF(1)
2	Database statistics		STAT(1), MON(1), PERF(1)
3	Accounting		ACCT(1), PERF(2)
4	Start/modify trace	DB2_COMMAND, RECORDDESC	All
5	Stop trace	DB2_COMMAND, RECORDDESC	All
6	Read I/O start	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	ACCT(3,8), MON(3,8), PERF(4)
7	Read I/O completion	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	ACCT(3,8), MON(3,8), PERF(4)
8	Write I/O start	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	ACCT(3,8), MON(3,8), PERF(4)
9	Write I/O completion	INTENT, RECORDDESC, SECURITY_EVENT	ACCT(3,8), MON(3,8), PERF(4)
10	Synchronous write I/O start	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	PERF(4)
11	Validation exit call results		PERF(13)
12	Encode exit call results		PERF(13)
13	Hash scan input		PERF(8)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
14	End of hash scan		PERF(8)
15	Index scan input		PERF(8)
16	Insert input		PERF(8)
17	Sequential scan input		PERF(8)
18	Exit from index scan, sequential scan, or insert		PERF(8) and IFCID(15) or IFCID(16) or IFCID(17)
19	Decode exit call results		PERF(13)
20	Lock summary		PERF(6)
21	Lock detail		PERF(7)
22	Optimizer mini-plan generation	DB2_OBJECT*, PROGRAM, RECORDDESC, SECURITY_EVENT	PERF(3)
23	Start utility	DB2_OBJECT*, RECORDDESC, SECURITY_EVENT	AUDIT(8), PERF(10)
24	Change utility	DB2_OBJECT*, RECORDDESC, SECURITY_EVENT	AUDIT(8), PERF(10)
25	End utility	DB2_OBJECT*, RECORDDESC, SECURITY_EVENT	AUDIT(8), PERF(10)
26	Sort work file obtained		PERF(3,9)
27	Sort new run		PERF(3,9)
28	Sort runs created		PERF(3,9)
29	EDM I/O start	SECURITY_EVENT	PERF(4)
30	EDM I/O end	SECURITY_EVENT	PERF(4)
31	EDM pool not large enough		PERF(1)
32	Start wait for log manager	INTENT	ACCT(3,8), MON(3,8), PERF(5)
33	End wait for log manager	RECORDDESC	ACCT(3,8), MON(3,8), PERF(5)
34	Log manager read I/O start	DSN, INTENT, RECORDDESC, SECURITY_EVENT	PERF(5)
35	Log manager read I/O completion	INTENT, RECORDDESC, SECURITY_EVENT	PERF(5)
36	Start wait for log manager non-I/O	RECORDDESC	PERF(5)
37	End wait for log manager non-I/O	RECORDDESC	PERF(5)
38	Log manager write active log I/O start	DSN, INTENT, RECORDDESC, SECURITY_EVENT	PERF(5), GLOB(3)
39	Log manager write active log I/O completion	DSN, INTENT, RECORDDESC, SECURITY_EVENT	PERF(5)
40	Log manager write archive log I/O start	DSN, INTENT, RECORDDESC	PERF(5)
41	Log manager write archive log I/O completion	INTENT, RECORDDESC	PERF(5)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
42	Checkpoint start		PERF(1)
43	Checkpoint completion		PERF(1)
44	IRLM suspend entry		ACCT(3,8), MON(3,8), PERF(6)
45	IRLM suspend exit		ACCT(3,8), MON(3,8), PERF(6)
46	Synchronous EU switch		PERF(11), GLOB(3)
47	SRB execution unit started		PERF(11), GLOB(3)
48	SRB execution unit completed		PERF(11), GLOB(3)
49	TCB execution unit started		PERF(11), GLOB(3)
50	TCB execution unit completed		PERF(11), GLOB(3)
51	Shared latch resume		ACCT(3,8), MON(3,8), PERF(11), GLOB(3)
52	Shared latch suspend entry		ACCT(3,8), MON(3,8), PERF(11), GLOB(3)
53	End describe		PERF(3)
54	Lock contention information		
55	Set current SQLid	DB2_SQLID, RECORDDESC	AUDIT(7), PERF(3)
56	Exclusive latch suspend		ACCT(3,8), MON(3,8), PERF(11), GLOB(3)
57	Exclusive latch resume		ACCT(3,8), MON(3,8), PERF(11), GLOB(3)
58	SQL call completion		PERF(3)
59	SQL fetch		PERF(3)
60	SQL select		PERF(3)
61	SQL del/insert/update	SECURITY_EVENT	PERF(3)
62	SQL auth/ddl/lock	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	PERF(3)
63	SQL statement bind	DB2_COMMAND, RECORDDESC, SECURITY_EVENT	PERF(3)
64	SQL prepare		PERF(3)
65	SQL open cursor		PERF(3)
66	SQL close cursor		PERF(3)
67	Accounting collection beginning		PERF(14)
68	Abort entry		PERF(2), GLOB(3)
69	Abort exit		PERF(2), GLOB(3)
70	Commit entry		PERF(2), GLOB(3)
71	Commit exit		PERF(2), GLOB(3)
72	Create thread entry		PERF(2), GLOB(3)
73	Create thread exit		PERF(2), GLOB(3)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
74	Terminate thread entry		PERF(2), GLOB(3)
75	Terminate thread exit		PERF(2), GLOB(3)
76	End of memory entry		PERF(1), GLOB(3)
77	End of memory exit		PERF(1), GLOB(3)
78	End of task entry		PERF(1)
79	End of task exit		PERF(1)
80	Establish exits entry		PERF(2), GLOB(3)
81	Establish exits exit		PERF(2), GLOB(3)
82	Identify entry		PERF(2), GLOB(3)
83	Identify request	DB2_SECAUTHID, DB2_SQLID, SECURITY_EVENT, USER, GROUP, RECORDDESC, SECLABEL, UTOKEN*	AUDIT(7), PERF(2), GLOB(3)
84	Prepare entry		PERF(2), GLOB(3)
85	Prepare exit		PERF(2), GLOB(3)
86	Signon entry		PERF(2), GLOB(3)
87	Signon request	DB2_SECAUTHID, DB2_SQLID, SECURITY_EVENT, USER, GROUP, RECORDDESC, SECLABEL, UTOKEN*	AUDIT(7). PERF(2), GLOB(3)
88	Sync start		PERF(2), GLOB(3)
89	Sync start		PERF(2), GLOB(3)
90	DB2 command start	DB2_COMMAND, RECORDDESC	PERF(10)
91	DB2 command completion	RECORDDESC	PERF(10)
92	AMS command start	DB2_COMMAND, RECORDDESC	PERF(3)
93	Suspend		PERF(11), GLOB(3)
94	Resume		PERF(11), GLOB(3)
95	Sort entry		PERF(3,9)
96	Sort exit		PERF(3,9)
97	AMS command completion	DB2_COMMAND, RECORDDESC	PERF(3)
98	Getmain/freemain entry		PERF(12)
99	Getmain/freemain exit		PERF(12)
100	Pool expansion/ contraction entry		PERF(12)
101	Pool expansion/ contraction exit		PERF(12)
102	Short on storage on		PERF(1)
103	Short on storage off		PERF(1)
104	Log data set DSID lookup info for other records	DSN, RECORDDESC	PERF(5)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
105	DBID/OBID lookup info needed for other records	DB2_OBJECT*	STAT(1), PERF(1,4,6,7, 8,10,13)
106	System parameters at startup	RECORDDESC	STAT(1), ACCT(1), MON(1), PERF(1,2,3,4, 5,6,7,8,9, 10,11,12,13, 14), GLOB(1,2,3,4)
107	Open/close table space	DB2_OBJECT*, RECORDDESC, SECURITY_EVENT	PERF(1,4,6,7, 8,10,13)
108	Bind/rebind start		PERF(10)
109	Bind/rebind completion		PERF(10)
110	Free beginning		PERF(10)
111	Free end		PERF(10)
112	Successful plan allocation allied threads		PERF(3)
113	Successful allocation system agents		PERF(11)
114	Begin read I/O archive	DSN, INTENT, RECORDDESC	PERF(5), GLOB(3)
115	End read I/O archive DASD	INTENT, RECORDDESC	PERF(5), GLOB(3)
116	End read I/O archive tape	INTENT, RECORDDESC	PERF(5), GLOB(3)
117	Start archive read		INTENT
118	Archive read completion	INTENT, RECORDDESC	ACCT(3,8), MON(3,8), PERF(5), GLOB(3)
119	Start BSDS write	DSN, INTENT, RECORDDESC	PERF(5)
120	BSDS write completion	INTENT, RECORDDESC	PERF(5)
121	Thread level entry into DB2		PERF(14)
122	Thread level exit from DB2		PERF(14)
123	SRV generated records		IFCID(123)
124	SQL statement record via IFI		MON(1,9)
125	Multiple index access path selection		PERF(8)
126	Buffer log writes		PERF(30)
127	Begin wait for I/O by another agent		ACCT(3,8), MON(3,8), PERF(4)
128	End wait for I/O by another agent		ACCT(3,8), MON(3,8), PERF(4)
129	Log CI record via reads request of ifi		MON(1)
130	Index logging		GLOB(4)
131	Used by utilities		GLOB(2)
132	DBET Changes		GLOB(1)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
133	EDM service		GLOB(2)
134	EDM service		GLOB(1)
135	Work file alloc/delete block		GLOB(5)
136	SQL parse		GLOB(5)
137	Path		GLOB(5)
138	EDM service		GLOB(1)
139	EDM service		GLOB(2)
140	Authorization failed	DB2_COMMAND, DB2_OBJECT*, INTENT, SECURITY_EVENT, USER, GROUP, RECORDDESC, SECLABEL, UTOKEN*	AUDIT(1)
141	Grant/revoke	DB2_COMMAND, DB2_OBJECT_TYPE, RECORDDESC, SECURITY_EVENT	AUDIT(2)
142	Create/drop/alter audited table	DB2_COMMAND, DB2_OBJECT*, USER, GROUP, INTENT, RECORDDESC, SECLABEL, SECURITY_EVENT, UTOKEN*	AUDIT(3)
143	First change (write) audited object	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	AUDIT(4)
144	First access (read) audited object	DB2_OBJECT*, INTENT, RECORDDESC, SECURITY_EVENT	AUDIT(5)
145	DML audit log	DB2_COMMAND, DB2_OBJECT*, INTENT, PROGRAM, RECORDDESC, SECURITY_EVENT	AUDIT(6)
146	Installation audit record		AUDIT(9)
147	Active thread snapshot		MON(1)
148	Active thread detail		MON(1)
149	All lock holders of a resource		MON(1)
150	All locks for a user		MON(1)
151	Installation accounting information		ACCT(4)
152	Installation statistics		STAT(2)
153	Installation performance exception		PERF(1)
154	Installation performance		PERF(15)
155	Installation monitoring		MON(4)
156	Installation serviceability		GLOB(6)
157	DRDS requesting site data		PERF(16)
158	DRDS responding site data		PERF(16)
159	DRDS conversation mgr interactions		PERF(16)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
160	DC requesting agent data		PERF(16)
161	DC responding agent data		PERF(16)
162	DTM requesting agent data		PERF(16)
163	DTM responding agent data		PERF(16)
164	VTAM exits to DB2		GLOB(7)
165	VTAM macro calls/returns		GLOB(7)
166	Buffer sent/received		GLOB(7)
167	Conversation allocation request		PERF(16)
168	Distributed SQL statement		GLOB(8)
169	Distributed authid translation	RECORDDESC	AUDIT(7)
170	Begin wait for EU switch		ACCT(3,8), MON(3,8)
171	End wait for EU switch		ACCT(3,8), MON(3,8)
172	Deadlock data		STAT(3), PERF(6)
173	Dynamic SQL exceeds ASUTIME	RECORDDESC	PERF(3), STAT(4)
174	Begin archive log mode(quiesce) wait		ACCT(3,8), MON(3,8), PERF(2), GLOB(3)
175	End archive log mode(quiesce) wait		ACCT(3,8), MON(3,8), PERF(2), GLOB(3)
177	Successful package allocation	DB2_OBJECT*, PROGRAM, RECORDDESC, SECURITY_EVENT	PERF(3)
178	Start DSNJW117 exit routine		STAT(30,31,32), PERF(30,31,32), GLOB(30,31,32), ACCT(30,31,32), AUDIT(30,31,32), MON(30,31,32)
179	End DSNJW117 exit routine		STAT(30,31,32), PERF(30,31,32), GLOB(30,31,32), ACCT(30,31,32), AUDIT(30,31,32), MON(30,31,32)
180	DSS communication buffers		GLOB(9)
181	DDM level 6B objects		GLOB(9)
182	DDM RDS/SCC interface data		GLOB(9)
183	DRDS RDS/SCC interface data	DB2_OBJECT*, PROGRAM, RECORDDESC	PERF(16)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
184	Decrypted communication buffers		GLOB(9)
185	Changed data capture		MON(6)
186	MEPL trace		IFCID(186)
187	Accounting class 5 flag		ACCT(5), MON(5)
188	CDC performance record		STAT(30,31,32), PERF(30,31,32), GLOB(30,31,32), ACCT(30,31,32), AUDIT(30,31,32), MON(30,31,32)
189	Activate 5FAC diagnostic logrec		
190	Hybrid join overflows		GLOB(5)
191	DDM level		STAT(4)
192	DDM header error		STAT(4)
193	COMMIT/ ROLLBACK mismatch		STAT(4)
194	Invalid SNA FMH-5 received		STAT(4)
195	DRDS exception		STAT(4)
196	Lock timeout		STAT(3), PERF(6)
198	Buffer mgr getpage/setwrite trace		IFCID(198)
199	Buffer mgr data set lstats trace		STAT(8), MON(1)
200	Accounting - nesting		None
201	Alter buffer pool command		PERF(10)
202	Dynamic zparm bufferpool information		STAT(1), MON(1)
203	Heuristic decision		STAT(4)
204	Partner cold start detected		STAT(4)
205	Incorrect logname or sync parms on warm start		STAT(4)
206	SNA Compare States protocol error		STAT(4)
207	Heuristic damage detected during SNA exchange		STAT(4)
208	SNA Synchpoint protocol error		STAT(4)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
209	Synchpoint communication failure		STAT(4)
210	LOGNAME changed on WARM START		STAT(4)
211	Make/Release/ Change Claim request information		PERF(17)
212	Drain/Release Claim request information		PERF(17)
213	Begin wait for a drain lock		ACCT(3,8), MON(3,8), PERF(6,17)
214	End wait for a drain lock		ACCT(3,8), MON(3,8), PERF(6,17)
215	Begin wait for claim count to go to zero		ACCT(3,8), MON(3,8), PERF(17)
216	End wait for claim count to go to zero		ACCT(3,8), MON(3,8), PERF(17)
217	Storage Pool Detail		GLOB(10)
218	Commit_LSN summary record		PERF(6)
219	Utility LISTDEF	RECORDDESC	AUDIT(8), PERF(10)
220	Utility data set close	DSN, INTENT, RECORDDESC, SECURITY_EVENT	AUDIT(8), PERF(10)
221	Degree of parallelism of a parallel group		PERF(8)
222	Number of rows processed by a parallel group		PERF(8)
223	Commit_LSN detail record		PERF(7)
224	Data Manager Select Procedure bypass trace		IFCID(224)
225	Storage Pool Summary		STAT(6)
226	Begin Wait due to page latch contention		ACCT(3,8), MON(3,8), PERF(4)
227	End Wait due to page latch contention		ACCT(3,8), MON(3,8), PERF(4)
228	Start archive tape unit deallocation wait		PERF(5), GLOB(3)
229	End archive deallocation wait		PERF(5), GLOB(3)
230	Data sharing global statistics		STAT(5), MON(1)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
231	Parallel tasks detail record		PERF(8)
232	Accounting class 2 ifcid		ACCT(2,7), MON(1,7)
233	Start/end call to user routine		PERF(3)
234	Calling agent authorization id		DB startup
235	Conditional restart data loss		STAT(4)
236	XLN protocol error		STAT(4)
237	Set current degree		PERF(3)
238	Error detected during DB2 restart		STAT(4)
239	Package/dbrm accounting overflow information		ACCT(1)
240	Accounting class 7 IFCid		ACCT(7), MON(7)
241	Accounting class 8 IFCid		ACCT(8), MON(8)
242	Begin wait for a stored procedure		ACCT(3,8), MON(3,8)
243	End wait for a stored procedure		ACCT(3,8), MON(3,8)
244	Stored Procedure Parameter List		PERF(32)
245	Stored Procedure Parameter List		PERF(32)
246	Stored Procedure Cache Table		PERF(32)
247	Input host variable tracing		GLOB(5)
248	Output host variable tracing		GLOB(5)
249	EDM pool invalidate dbd		PERF(20), GLOB(5)
250	Connect/disconnect of a group buffer pool		STAT(3), PERF(20)
251	Pageset/partition P-lock(negotiation) request		PERF(20)
252	Beginning of XES request		GLOB(3)
254	Backing cache structure stats		STAT(5), MON(2)
255	Buffer refresh due to cross-invalidation		PERF(21)
256	Alter group bufferpool command		PERF(10,20)

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
257	IRLM notify request detail		PERF(20)
258	Extend data set	DB2_OBJECT*, DSN, INTENT, RECORDDESC, SECURITY_EVENT	STAT(3)
259	Page P-lock request(or negotiation) request		PERF(21)
260	End of XES request		GLOB(3)
261	Group buffer pool checkpoint		STAT(3), PERF(20)
262	Group buffer pool castout threshold		STAT(3), PERF(20)
263	Pageset and partition castout statistics		PERF(21)
265	SCA access request begin		GLOB(3)
266	SCA access request end		GLOB(3)
267	CF rebuild start event		STAT(4), PERF(20), GLOB(3)
268	CF rebuild end event		STAT(4), PERF(20), GLOB(3)
269	Trusted connection established/reused	GROUP, RECORDDESC, SECLABEL, SRCIP, USER, UTOKEN*	AUDIT(10)
270	Trusted context created/altered	DB2_COMMAND, RECORDDESC	AUDIT(10)
271	Row and column access control	`DB2_COMMAND, DB2_OBJECT_TYPE, RECORDDESC`	
272	Associate locators statement info		PERF(3)
273	Allocate cursor statement info		PERF(3)
274	Input SQLDA/host variable ctrl blk		PERF(32)
275	Output SQLDA/host variable ctrl blk		PERF(32)
276	Input SQLDA/transition variable		PERF(32)
277	Routine get storage		PERF(32)
278	Routine free storage		PERF(32)
280 - 298	Error simulation		
299	DRDA exception		
300 - 304	Error simulation		
305	Check constraint		PERF(8)
306	Log records via IFI reads		MON(2)
307 - 310	Error simulation		

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
311	Global temporary tables		PERF(3,8)
312	DCE authorization (obsolete)		PERF(8)
313	Long running URs at checkpoint		STAT(3)
314	Authorization exit access control action	USER, GROUP, RECORDDESC, SECLABEL, SECURITY_EVENT, UTOKEN*	PERF(22)
316	Prepared statement cache stats		MON(1)
317	Prepared statement cache statement		MON(1)
318	Prepared statement cache switch		None
319	Kerberos identity	RECORDDESC, SRCIP	AUDIT(7)
320	Debug messages		
321	Begin force-at-commit		PERF(2)
322	End force-at-commit		PERF(2)
323	Predictive governor serviceability		
324	Function resolution trace		PERF(3)
325	End of trigger activation		PERF(3)
326	EU switch dump trigger-internal only		None
327	LE runtime diagnosis		PERF(23)
328	Built in function service trace		
329	Asynch IXLCACHE/ IXLFCOMP requests		ACCT(3), MON(3), PERF(21)
330	Active log shortage situation		STAT(3)
331	Locator service		PERF(32)
332	TransCSO service		PERF(32)
333	Traverse CSO		PERF(32)
334	DRDA exceptions for scrollable cursor		PERF(32)
335	System event stalled notification		STAT(3)
336	Output CCSID cntl block		
337	Lock escalation occurrences		PERF(6), STAT(3)
338	Storage analysis		
339	Package detail switch		
340	SQLCODE trace		

Table 522. SMF record type 100, 101, and 102: DB2 Performance and Audit SUBTYPEs (continued)

Subtype	Meaning	Specific field support	Trace class or IFCID
341	Incremental bind for special register		
342	WF/TD usage per agent		PERF(32)
343	MAXTEMPS zparm limit for agent is exceeded	RECORDDESC	PERF(3), STAT(4)
344	SP/UDF function entry/exit point	RECORDDESC	GLOB(11)
345	SP/UDF function data point	RECORDDESC	GLOB(11)
346	Active package detail	RECORDDESC	
347 - 349	Serviceability IFI trace		
350	SQL bind full statement	DB2_COMMAND, RECORDDESC, SECURITY_EVENT	PERF(3,32)
351	Begin TCP/IP LOB materialization	RECORDDESC	ACCT(3,8)
352	End TCP/IP LOB materialization	RECORDDESC	ACCT(3,8)

Table 523. SMF record type 103: IBM HTTP Server SUBTYPEs

Subtype	Meaning	Specified field support
1	IBM HTTP Server configuration data	
2	IBM HTTP Server performance data	
361	Audit administrative authorities	`DB2_COMMAND`, `DB2_OBJECT_TYPE`, `INTENT`, and `RECORDDESC`
362	Begin audit trace with `AUDITPOLICY`	`DSN`, `RECORDDESC`

Table 524. SMF record type 110: CICS Records SUBTYPEs

Subtype	Meaning
0	CICS Journaling data
1	CICS Monitoring data. The CICS monitoring records have four subclasses: • Dictionary • Performance • Exception • Transaction resource
2	CICS Statistics
3	CICS Shared temporary queue server
4	CICS Coupling facility data server

Table 524. SMF record type 110: CICS Records SUBTYPEs (continued)

Subtype	Meaning
5	CICS Named counter sequence number

Table 525. SMF record type 115: MQSeries Statistics SUBTYPEs

Subtype	Meaning
1	MQSeries® log statistics
2	MQSeries performance information

Table 526. SMF record type 119: Connectivity Statistics SUBTYPEs

Subtype	Meaning
1	TCP Connection Initiation
2	TCP Connection Termination
3	FTP Client Transfer Completion
4	TCP/IP profile event record
5	TCP/IP Statistics
6	Interface Statistics
7	Server Port Statistics
8	TCP/IP Stack Start/Stop
10	UDP Socket Close
20	TN3270 Server SNA Session Initiation
21	TN3270 Server SNA Session Termination
22	TSO Telnet Client Connection Initiation
23	TSO Telnet Client Connection Termination
48	CSSMTP Configuration
49	CSSMTP Connection
50	CSSMTP Mail
51	CSSMTP Spool
52	CSSMTP Statistics
70	FTP Server Transfer Completion
72	FTP Server Login Failure
73	IPsec IKE Tunnel Activation/Refresh
74	IPsec IKE Tunnel Deactivate/Expire
75	IPsec Dynamic Tunnel Activation/Refresh
76	IPsec Dynamic Tunnel Deactivation
77	IPSec Dynamic Tunnel Added
78	IPsec Dynamic Tunnel Remove
79	IPsec Manual Tunnel Activation
80	IPsec Manual Tunnel Deactivation

Table 527. SMF record type 120: Websphere AS Performance Statistics SUBTYPEs

Subtype	Meaning
1	Websphere AS Server Activity
2	Websphere AS Container Activity
3	Websphere AS Server Interval
4	Websphere AS Container Interval

SYSNAME

The SYSNAME field specifies the name of the system. This value is used as part of the SAF resource name in the IP_PORT_RESOURCE and IP_NETACCESS_RESOURCE fields for SMF records of type 119

SYSPLEX

The name of the sysplex the SYSTEM is a part of (if applicable).

SYSTEM

The name of the system (the SMF system id, which is four characters long). Found in all record types.

SYSTYPE

Operating system type. This field is found in all record types.

Note: The output values for this field are not identical to the SELECT/EXCLUDE values; also, the default output size of this field is three characters; use an overriding length of nine to get the full output.

Table 528 lists the possible SYSTYPE values (in increasing sort order).

Table 528. SMF record SYSTYPE field - SELECT/EXCLUDE and Output values

SELECT/EXCLUDE value	Output value	Meaning
VM	VM	VM
VS2	VS2	OS/VS2
SP2 XA	SP2 (XA)	MVS/XA
SP3 ESA	SP3 (ESA)	MVS/ESA SP3
SP4 SP5	SP4 (ESA)	MVS/ESA SP4 or SP5

TERMINAL

Terminal id. This field is found in the following record types:

- Job Initiation and Accounting records (SMF record types 20, 30 and 32)
- RACF processing and R_auditx records (SMF record types 80 and 83
- HSM function statistics records
- Telnet server TCP/IP records (SMF record types 118 and 119)
- CICS subrecords (SMF record type 110, subtype 1, class 3)

The value of TERMINAL is derived using the job tag system for data set, ICF catalog activity records, RACF processing, and audit records for data sets and UNIX file system activity records (SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65 and, 66, 80, 83 and 92).

TIME

Time of day the record was written. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Time fields" on page 904.

TRANSACTION

For CICS monitoring performance subrecords (SMF 110, subtype 1, subclass 3), this field returns the name of the transaction that was run. If this information is not available, this field is not reported.

TSOCMD

A string containing a TSO command name. This repeated field is only found in SMF record type 32 (TSO/E User Work Accounting), and only contains those TSO commands accounted by the installation; all other commands are collected as ***OTHER. This field can be combined with the TSOCMDCNT field.

TSOCMDCNT

A repeated field containing the number of times a given TSO command was executed. This field can only be used for output and should be combined with the TSOCMD field.

TYPE

SMF numerical record type. This field is found in all record types. When used in SELECT/EXCLUDE processing, this field is used to select types and subtypes; for output, these fields are separated in TYPE and SUBTYPE.

For SELECT/EXCLUDE processing, each record type can be further specified by a list of *subtypes*, as shown in the following examples:

```
SELECT TYPE=(20, 30, 32, 80, 83)
SELECT TYPE=(20, 30(1, 3, 4, 6), 80, 83(1))
SELECT TYPE<>(20 30(5) 80)
```

For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

UNITTYPE

This field can be used to select or output the device type used. It is found in data set activity records (SMF record types 14, 15, 62 and 64), ICF Catalog Activity records (SMF record type 61, 65, and 66), and Accounting records (SMF record type 30). In SMF record type 30, the unit type is not available in all subtypes, and is only available for started tasks if detail recording is on. This value can be verified using the DETAIL field of NEWLIST TYPE=SMFOPT.

Table 529 lists the possible UNITTYPE values.

Table 529. SMF record UNITTYPE field - possible values

UNITTYPE value	Meaning
3350	3350 DASD Unit
3380	3380 DASD Unit
3390	3390 DASD Unit
3400	3400 Tape Unit

Table 529. SMF record UNITTYPE field - possible values (continued)

UNITTYPE value	Meaning
3480	3480 Tape Unit
3490	3490 Tape Unit
9345	9345 DASD Unit
DASD	Unknown (output) or any (SELECT) type of DASD Unit
TAPE	Unknown (output) or any (SELECT) type of Tape Unit
????	Unknown unit type (not tape or DASD) (output-only)

Note: There is a slight difference between SELECT/EXCLUDE processing and output values: TAPE and DASD match any tape or DASD unit in SELECT/EXCLUDE processing, but is only output for an unknown type of tape or DASD unit; the value '**????**' cannot be used for SELECT/EXCLUDE processing, but is output-only. For SELECT/EXCLUDE processing, only the =, <>, and ¬= relational operators can be used.

Note: UNITTYPE is a repeated field. In the current version of Security zSecure, this repeated field can contain duplicate unit types for some record types.

UNIX_ACCESS_ALLOWED

This field of length 3 is only found in RACF processing records (SMF record type 80). It corresponds with RACF_SECTION(269), *Access allowed*. The three characters might be "-" (access not allowed); the first character can alternatively be "r" for "Access read allowed", the second "w" for "Access write allowed", and the third "x" for "Access execute allowed". See also UNIX_ACCESS_USED.

The SELECT/EXCLUDE syntax for this field is the same as for the NEWLIST TYPE=UNIX field ATTR (see "Formatting UNIX file type, attribute, and audit flag fields" on page 823). For example, you can select on "execute allowed" with UNIX_ACCESS_ALLOWED='+x'M. If access for "u" specifically is asked, an extra check is done if the corresponding UNIX_ACCESS_ORIGIN value is "user"; and likewise "g" matches only if that field is "group" and "o" when it is "other". For example, you can select on "write access allowed via the other bits" with UNIX_ACCESS_ALLOWED='o+w'M.

UNIX_ACCESS_FILENAME

UNIX_ACCESS_FILENAME shows the name of the file or directory to which access was attempted. It was verified whether the access was allowed.

This field is found in the following record types:

- RACF processing records (SMF record type 80)
- Security audit event records (SMF record type 83, subtype 5 and 6)

The `UNIX_ACCESS_FILENAME` combines information from extended-length relocate sections 263, 264, and 298. If a CKFREEZE file is present, the information in it is consulted for translating file identifiers into full path names and the like.

A CKFREEZE file contains data from a particular point in time. For example, if a `RENAMEF` event is enriched based on a CKFREEZE system snapshot from slightly before the event, the record results probably yield the *old* file name.

For some events, `UNIX_ACCESS_FILENAME` is identical to `UNIX_FILENAME`. For other events, `UNIX_ACCESS_FILENAME` is the name of the directory to which access was

attempted as a result of requesting access to UNIX_ACCESS_FILENAME. UNIX_ACCESS_FILENAME is the last qualifier of UNIX_ACCESS_PATHNAME.

The default output format for this field shows the first 256 characters of the file name are shown in the output which can exceed available space on the output line. To include the full file name, use the following format specification in CARLa scripts: `unix_access_filename(0,wrap)`

UNIX_ACCESS_INTENT

This field of length 4 is found only in RACF processing records (SMF record type 80) , NFS audit statistics records (SMF record type 42 subtype 26), and ACF2 OMVS CHECK_ACCESS records. For RACF, it corresponds with the bits in RACF_SECTION(267), "Requested access". For ACF2, it corresponds with the bits in SMFRQACC. The first character of the field can be "d" (directory search access intended) or "-" (no directory search access intended), although for DIRSRCH events, the character usually reads "-". The second character can be "r" (read access intended) or "-" (no read access intended). The third character can be "w" (write access intended) or "-" (no write access intended). The fourth character can be "x" (execute access intended) or "-" (no execute access intended).

Select/Exclude syntax for the UNIX_ACCESS_INTENT field is like the NEWLIST TYPE=UNIX field EXTATTR syntax, with characters "drwx" replacing "apsl". For example, you can select on the presence of the "r" and "w" bits with UNIX_ACCESS_INTENT='+rw'M. See “Formatting UNIX file type, attribute, and audit flag fields” on page 823 for the (extended) EXTATTR syntax supported for SELECT/EXCLUDE processing.

UNIX_ACCESS_ORIGIN

This character field of length 10 is found only in RACF processing records (SMF record type 80). It corresponds with the value of RACF_SECTION(268), "Access type (bits used to make access check)". The recognized values for this field are "user" (user bits used), "group" (group bits used), "other" (other bits used), "no" (no bits present), "user ACL" (user ACL entry used), "group ACL" (group ACL entry used), "no ACL" (an ACL entry exists but it could not be retrieved), "restricted" (other bits not used because of the RACF user's RESTRICTED attribute), and "n/a" (the security label of the user is insufficient for access). Unrecognized values are printed in decimal.

The SELECT/EXCLUDE syntax for this field allows a list of values, e.g., UNIX_ACCESS_ORIGIN=('user'c,'group'c,'other'c). Note that you must specify that case is to be kept. Note that values of "user", "group" and "other" can also be selected on in combination with UNIX_ACCESS_ALLOWED and UNIX_ACCESS_USED--see there. For backwards compatibility, the one-character selection codes 'u'c, 'g'c, 'o'c, and - are still supported for now, too; these are interpreted as 'user', 'group', 'other' and 'no', respectively.

UNIX_ACCESS_PATHNAME

UNIX_ACCESS_PATHNAME shows the path name of the file or directory to which access was attempted. It was verified whether the access was allowed. The field is found in the following record types.

- RACF processing records (SMF record type 80)
- Security audit event records (SMF record type 83, subtype 5 and 6)

For RACF, UNIX_ACCESS_PATHNAME combines information from extended-length relocate sections 263, 264, and 298. If a CKFREEZE is present, the information in it is consulted for translating file identifiers into full path names and the like.

A CKFREEZE file denotes a particular point in time. For example, if a RENAMEF event is enriched based on a CKFREEZE system snapshot from slightly before the event, this field value will probably yield the full *old* path name.

For some events, UNIX_ACCESS_PATHNAME is identical to UNIX_PATHNAME. For other events, UNIX_ACCESS_PATHNAME reflects the directory to which access was attempted as a result of requesting access to UNIX_PATHNAME. In the latter case, UNIX_PATHNAME is the concatenation of UNIX_ACCESS_PATHNAME and UNIX_FILENAME.

The default output format for this field shows the first 256 characters of the file name are shown in the output which can exceed available space on the output line. To include the full path name, use the following format specification in CARLa scripts: `unix_access_pathname(0,wrap)`

UNIX_ACCESS_USED

This field of length 3 is only found in RACF processing records (SMF record type 80). It combines information from RACF_SECTION(267), "Requested access" and RACF_SECTION(269), "Access allowed". It indicates which kinds of access were both intended and allowed. Its contents are similar to those of the UNIX_ACCESS_ALLOWED field, but the corresponding character for each type of access is set to "-" if the access was not requested.

The SELECT/EXCLUDE syntax for this field is the same as for the NEWLIST TYPE=UNIX field ATTR (see “Formatting UNIX file type, attribute, and audit flag fields” on page 823). You can select on "write access" with UNIX_ACCESS_USED='+w'M. If access for "u" specifically is asked, a check is done if the corresponding UNIX_ACCESS_ORIGIN value is "user"; and likewise "g" matches only if that field is "group" and "o" when it is "other". For example you can select on "successfully reading your own file" with UNIX_ACCESS_USED='u+r'M.

If UNIX_ACCESS_USED is "---" a violation has occurred, unless UNIX_ACCESS_ORIGIN indicates that the access check could not be performed ("no ACL") or does not apply ("no").

UNIX_FILENAME

`UNIX_FILENAME` shows the name of the file or directory to which access was requested. This field is found in the following record types:

- RACF processing records (SMF record type 80)
- OpenMVS File System activity records (SMF records type 92)
- TCP/IP statistics records (SMF record types 118 and 119, FTP-related subtypes only)
- CSSMTP configuration records (SMF record type 119 subtype 48)
- Security audit event records (SMF record type 83, subtype 5 and 6)
- NFS audit statistics records (SMF record type 42 subtype 26)

`UNIX_FILENAME` is a repeated field for RACF which combines information from extended-length relocate sections 263, 264, 270, 271, and 298. If a `CKFREEZE` file is present, the information in it is consulted for translating file identifiers into full path names and the like.

With FACCESS events, the new file name precedes the old file name.

With SMF record types 92, 118, and 119 (except type 119 subtype 48), the UNIX_FILENAME field contains a single file name at most.

A CKFREEZE file contains data from a particular point in time. For example, if a RENAMEF event is enriched based on a CKFREEZE system snapshot that was taken slightly before the event, the data in the UNIX_FILENAME field will probably yield the *old* file name. UNIX_FILENAME is the last qualifier of UNIX_PATHNAME.

The default output format for this field shows the first 256 characters of the file name which can exceed available space on the output line. To include the full file name, use the following format specification in CARLa scripts: unix_filename(0,wrap).

UNIX_FILETYPE

This field is found in RACF processing records (SMF record type 80) that contain a file audit ID, NFS audit statistics records (SMF record type 42 subtype 26), and in UNIX File System activity records (SMF record type 92) containing an inode. It may contain the UNIX file type (see "TYPE" on page 1489). This is determined via a lookup to the UNIX file system. The field is empty if no CKFREEZE is present or if the CKFREEZE does not contain the required information. File audit ids in RACF processing records are contained in RACF_SECTION(264) and RACF_SECTION(271). This is not a repeated field; if both file audit id sections are present, the first match against the UNIX file system determines the result. Currently the file audit id is only available for files in an HFS. See also UNIX_PATHNAME.

UNIX_FUNCTION

This numeric field is only found in RACF processing records (SMF record type 80) , NFS audit statistics records (SMF record type 42 subtype 26), and in ACF2 OMVS records. The UNIX_FUNCTION field represents the USS Audit Function Code (found in RACF_SECTION(256) with RACF and found in SMFOEAFC with ACF2). The field one of the indications tabulated below of the operation which led to the creation of the SMF record. The UNIX_FUNCTION field can be compared with numbers and with indications (non-quoted strings), as in UNIX_FUNCTION=(mount, DUB, 19, '1A'x). Indications AFC_*nnn* cannot be used in comparisons. Use numbers *nnn* instead. For example, use 0 instead of AFC_0.

Table 530. SMF record UNIX_FUNCTION field - indicator values

Indication	Value	Description
access	1	Check file accessibility
acc_disc	97	Discard access rights
acc_recv	96	Receive access rights
acc_send	95	Send access rights
authcheck	94	Authority check
bind	91	Bind a name to a socket
chattr	59	Change file attributes
chaudit_a	37	Change auditor audit options
chaudit_u	2	Change user audit options
chdir	3	Change current working directory
chmod	4	Change file modes

Table 530. SMF record UNIX_FUNCTION field - indicator values (continued)

Indication	Value	Description
chmount	109	Change mount (with the NOSETUID operand)
chmount_setuid	110	Change mount (using the SETUID operand)
chown	5	Change owner and group of file
chroot	88	Change root directory
console	99	Console communication service
dub	6	Initialize a process
eaccess	113	Check file access for effective IDs
exec	7	Execute a file
fchattr	60	Change file attributes for open file
fchaudit_a	38	Change auditor audit options when file is open
fchaudit_u	8	Change user audit options when file is open
fchdir	87	Change working directory
fchmod	9	Change file modes when file is open
fchown	10	Change owner and group of file when open
getcwd	11	Get current working directory
getmnt	42	Get mount entry
getpsent	12	Get process entry
ioctl	41	Get path name
kill	13	Signal a process
lchattr	116	Change attributes of file, directory, or symbolic link
lchown	79	Change owner and group of a symbolic link
link	14	Link to a file
login	104	__LOGIN system call
lookup	39	Path name resolution
lstat	15	Get file status; do not resolve ending symlink
mkdir	16	Make a directory
mknod	17	Make a file node
mount	18	Mount a file system (using the NOSETUID operand)
mount_na	118	Mount no audit
mount_setuid	105	Mount a file system (using the SETUID operand)
mount_u	119	User mount
mount_una	120	User mount no audit
msgctl	62	Message control
msgget	63	Message obtain
msgrcv	64	Message receive
msgsnd	65	Message send
newgrp	98	Newgrp shell utility
nice	84	Change priority of a process
open	19	Open a file
opendir	20	Open a directory

Table 530. SMF record UNIX_FUNCTION field - indicator values (continued)

Indication	Value	Description
password	78	Verify password
pathconf	21	Get configurable path name variables
pfsctl	81	Control function for the physical file system
poe	115	Provide port of entry identifier
ptrace	22	Debug a process
quiesce	43	Quiesce a file system (with the NOSETUID operand)
quiesce_setuid	107	Quiesce a file system (using the SETUID operand)
readlink	23	Read a symbolic link
realpath	89	Resolve path name
remove	74	Remove
rename	24	Rename a file
rmdir	25	Remove a directory
semctl	66	Semaphore control
semget	67	Get set of semaphores
semop	68	Semaphore operations
serv_init	100	WLM service Console communication service
setegid	26	Set effective GID
seteuid	27	Set effective UID
setfacl	111	Set, remove, or change ACLs
setfsecl	114	Set file seclabel
setgid	28	Set real/saved and/or effective GID
setpriority	83	Set process scheduling priority
setregid	71	Set real and/or effective GID
setreuid	85	Set real and/or effective UID
setrlimit	82	Set maximum resource consumption
setuid	29	Set real/saved and/or effective UID
set_gid	77	Set supplementary groups
set_mode	75	Set mode
set_msgqb	76	Set message queue maximum bytes
shmat	69	Shared memory attach
shmctl	70	Shared memory control
shmget	72	Shared memory get
shutdown_reg	112	USS shutdown registration
sigaction	50	Change Osigset action
socket	92	Create an endpoint for communication
spawn	101	Spawn
stat	30	Get file status
statvfs	90	Get file system information
swap_serv	102	Swap services
symlink	31	Create a symbolic link

Table 530. SMF record UNIX_FUNCTION field - indicator values (continued)

Indication	Value	Description
thlmt	61	Set thread limit
thread_sec	93	Thread level security
truncate	80	Truncate a file
ttyname	40	Get path name of terminal
unavailable	117	Audit function code not available
undub_exit	35	Terminate a process
unlink	32	Remove directory entries (Delete a file)
unmount	33	Unmount a file system (with the NOSETUID operand)
unmount_setuid	106	Unmount a file system (using the SETUID operand)
unmount_u	121	User unmount
unmount_una	122	User unmount no audit
unquiesce	44	Unquiesce a file system (with the NOSETUID operand)
unquiesce_setuid	108	Unquiesce a file system (using the SETUID operand)
utime	34	Set file access/modification times
vcreate	51	Server create
vlink	55	Server link
vlookup	47	Server lookup
vmakedir	52	Server make directory
vreaddir	49	Server read directory
vreadwrite	48	Server read write
vregister	45	Server registration
vremove	57	Server remove
vremovedir	56	Server remove directory
vrename	58	Server rename
vresolvepn	46	Server resolve path name
vsetattr	54	Server set file attributes
vsymlink	53	Server symbolic link
wgetipc	73	Query IPC status
wlmc	103	WLM C and C++
write	36	Write to a file (Clear setid bits)
writev	86	Write on a file

UNIX_PATHNAME

UNIX_PATHNAME shows the path name of the file or directory to which access was requested. The field is supported in the following record types:

- RACF processing records (SMF record type 80)
- OpenMVS File System activity records (SMF records type 92)
- CSSMTP configuration records (SMF record type 119 subtype 48)
- NFS audit statistics records (SMF record type 42 subtype 26)

UNIX_PATHNAME is a repeated field for RACF which combines information from extended-length relocate sections 263, 264, 270, 271, and 298. With record

type 80 and with ACF2 OMVS records, it can have 1 or 2 entries of at most 1023 characters each. With RENAMEF events, the first entry is the old path name and the second entry is the new path name. On the other hand, with FACCESS events, the new path name precedes the old path name. With record types 92, 118, and 119 CSSMTP configuration records (SMF record type 119 subtype 48), the UNIX_PATHNAME field contains a single path name at most. If a CKFREEZE is present, then with RACF but not with ACF2, the information in it is consulted for translating file identifiers into full path names and the like. Note that a CKFREEZE denotes a particular point in time; e.g., if a RENAMEF event is enriched based on a CKFREEZE system snapshot from slightly before the event, this will probably yield the full *old* path name. The last qualifier of UNIX_PATHNAME is UNIX_FILENAME. For ACF2 OMVS records, the path names are usually relative.

The default output format for this field shows the first 256 characters of the file name are shown in the output which can exceed available space on the output line. To include the full path name, use the following format specification in CARLa scripts: `unix_pathname(0,wrap)`

UNIX_PROGRAM

UNIX program name. This field contains the first 16 bytes of the UNIX program path name run as a substep (through the UNIX exec service) within a job step. It is only found in SMF record type 30.

USER, USERID

SAF userid. This field is found in the following record types:

- DFSORT records (SMF record type 16)
- Job Initiation and Accounting records (SMF record types 20, 30 and 32)
- RACF processing and R_auditx records (SMF record types 80 and 83)
- NFS audit statistics records (SMF record type 42 subtype 26)
- z/OS Firewall Technologies records (SMF record type 109)
- CICS records (SMF record type 110)

  For CICS subrecords, USER returns the RACF userid that performed the CICS transaction.
- HSM function statistics records
- DB2 records (SMF record type 102) with subtypes/IFCids 83, 87, 140, 142, 269, and 314 if non-blank and non-null.
- CSSMTP client records (SMF record type 119) with subtypes 48, 50, and 51 if non-blank and non-null.

It is derived using the job tag system for data set and ICF catalog activity records (SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65 and 66).

Note: Some HSM function statistics records may contain the user id ****HSM***** or ***H*S*M*** (the second pseudo-userid starts with a leading zero). These are not SAF userids, but pseudo-userids generated by the HSM software.

To select a userid that is the target of a RACF command, use one of the RACFCMD_USER, RESOURCE or PROFILE fields instead. To select a userid that is the target of an ACF2 command, use ACF2_RULEKEY instead. The USER field describes the command-issuing user, not the target user.

UTOKEN

A string describing the contents of the User Security Token included in the following record types:

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

Because UTOKEN contains many fields, many of which need not be set, the output has the format `field1: value1; field2: value2`.

This field can only be used for output; to select all records with a UTOKEN field, use SELECT RELOCATE=53. To select on values contained in the UTOKEN field, use the following derived fields:

```
UTOKEN_FLAGS, UTOKEN_SESSION, UTOKEN_POE
UTOKEN_POECLASS, UTOKEN_SUSER, UTOKEN_SGROUP
UTOKEN_SNODE and UTOKEN_XNODE
```

Note: The values printed by the UTOKEN field are subject to change. Do not write applications that are dependent on the output of this field.

UTOKEN_FLAGS

This field describes the flags found in the User Security Token, which is included in the following record types:

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output. However, in most cases the UTOKEN field is more convenient for output.

Because many flags can be set at the same time, the default output of this field is in a condensed format; full output split into several lines can be requested using the EXPLODE output modifier, for example, UTOKEN_FLAGS(EXPLODE). The following table lists the UTOKEN_FLAGS values that can be used for SELECT/EXCLUDE processing; the condensed output; the exploded output; and the meaning.

Table 531. SMF record UTOKEN_FLAGS field - values for output processing

SELECT/EXCLUDE	Condensed	Exploded	Meaning
DEFAULT	... .D. ...	Default	Default user
ENCRYPTED	... ... C..	Encrypted	Token is encrypted
ERROR	... .E	Error	Token in error
LOG, LOGUSER	..L	Log user	User is logged (UAUDIT)
NJEUNKNOWN	... .N. ...	NJE Unknown	NJE unknown user
PRE19	... .<.	Pre 1.9	Created by pre 1.9 call
PRIVILEGED	P..	Privileged	Privileged user
PROPAGATE	... P.. ...	Propagate	Propagated ID values
REMOTE	... ..R ...	Remote	Remote job
SPECIAL	.S.	Special	User has special attribute
SURROGATE	... S.. ...	Surrogate	Surrogate job
TRUSTED	T..	Trusted	Trusted user
UNDEFINED	... .U. ...	Undefined	Undefined user

Table 531. SMF record UTOKEN_FLAGS field - values for output processing (continued)

SELECT/EXCLUDE	Condensed	Exploded	Meaning
WRITEDOWN	... ...W ...	WriteDown	MLS WriteDown

For SELECT/EXCLUDE processing, a list of values may be specified, e.g. SELECT UTOKEN_FLAGS=(SURROGATE,REMOTE,PROPAGATE). Only the =, <>, and ¬= relational operators can be used. With the = relational operator, the SELECT/EXCLUDE expression is true if any record's UTOKEN flags type matches any of the values specified; with the <> and ¬= relational operators, the SELECT/EXCLUDE expression is true if all of the record's UTOKEN flags types match none of the values specified.

Notes:

1. The condensed output is split into three parts: user attributes, job attributes, and token attributes.
2. The values printed by the UTOKEN_FLAGS field are subject to change. Do not write applications that are dependent on the output of this field.

UTOKEN_POE

This text field describes the Port-Of-Entry contained in the User Security token, which is included in the following record types:

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

UTOKEN_POE can be used for SELECT/EXCLUDE processing and for output. However, in most cases the UTOKEN field is more convenient for output. The Port-Of-Entry class is described with the UTOKEN_POECLASS field.

UTOKEN_POECLASS

This field describes the Port-Of-Entry class type contained in the User Security token, which is included in the folllowing record types:

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output. However, in most cases the UTOKEN field is more convenient for output. The Port-Of-Entry is described with the UTOKEN_POE field.

UTOKEN_POECLASS values are:

APPCPORT
CONSOLE
JESINPUT
SERVAUTH
TERMINAL

For SELECT/EXCLUDE processing, a list of values may be specified, e.g. SELECT UTOKEN_POECLASS=(TERMINAL,JESINPUT). The numeric value of the Port-Of-Entry class can be specified as well. Only the =, <>, and ¬= relational operators can be used. With the = relational operator, the SELECT/EXCLUDE expression is true if the record's Port-Of-Entry class

matches any of the values specified; with the <> and ¬= relational operators, the SELECT/EXCLUDE expression is true if the record's Port-Of-Entry class matches none of the values specified.

UTOKEN_POE_NETWORK

This text field describes the Port-Of-Entry Network contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field will be more convenient for output.

UTOKEN_SESSION

This field describes the session type contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field is more convenient for output.

The following table lists the UTOKEN_SESSION values that can be used for SELECT/EXCLUDE processing; the output values; and the meaning (XBM=eXternal Batch Monitor; NJE=Network Job Entry; RJE=Remote Job Entry).

Table 532. SMF record UTOKEN_SESSION field - values for output processing

SELECT/EXCLUDE	Output	Meaning
APPC	APPC	APPC
COMMAND	Command	Command
CONSOLE	Console	Console operator
EXTJOB EXTRDRJOB	Extrdr job	External reader job
EXTXBM EXTRDRXBM	Extrdr XBM	External reader XBM
INTJOB INTRDRJOB	Intrdr job	Internal reader job
INTXBM INTRDRXBM	Intrdr XBM	Internal reader XBM
MOUNT	Mount	Mount
NJEJOB	NJE job	NJE job
NJEOPER	NJE operator	NJE operator
NJESYSOUT	NJE sysout	NJE sysout
NJEUNKNOWN	NJE unknown user	NJE unknown user
NJEXBM	NJE XBM	NJE XBM
OMVSSRV OMVS	OMVSSRV	OMVSSRV
RJEJOB	RJE job	RJE job
RJEOPER	RJE operator	RJE operator

Table 532. SMF record UTOKEN_SESSION field - values for output processing (continued)

SELECT/EXCLUDE	Output	Meaning
RJEXBM	RJE XBM	RJE XBM
STC	STC	Started procedure
SYSTEM	System	System address space
TSO	TSO	TSO logon

For SELECT/EXCLUDE processing, a list of values may be specified, e.g. SELECT UTOKEN_SESSION=(NJEXBM,NJESYSOUT,NJEJOB). Only the =, <>, and ¬= relational operators can be used. With the = relational operator, the SELECT/EXCLUDE expression is true if the record's session type matches any of the values specified; with the <> and ¬= relational operators, the SELECT/EXCLUDE expression is true if the record's session types matches none of the values specified.

UTOKEN_SGROUP, UTOKEN_SGRP

This text field describes the connect group of the submitting user contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field is more convenient for output. See also the UTOKEN_SUSER, UTOKEN_SNODE, and UTOKEN_XNODE fields.

UTOKEN_SNODE

This text field describes the submitting node contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field is more convenient for output. See also the UTOKEN_SGROUP, UTOKEN_SUSER, and UTOKEN_XNODE fields.

UTOKEN_SUSER, UTOKEN_SUSR

This text field describes the submitting user contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).
- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field is more convenient for output. See also the UTOKEN_SGROUP, UTOKEN_SNODE, and UTOKEN_XNODE fields.

UTOKEN_XNODE

This text field describes the execution node contained in the User Security token, which is included in the following record types.

- All RACF processing records (SMF record types 80 and 83 subtype 1).
- In several DB2 subtypes (SMF record type 102).

- In CSSMTP subtypes (SMF type 119 subtype 48 records).

It can be used for SELECT/EXCLUDE processing and for output; however, in most cases the UTOKEN field is more convenient for output. See also the UTOKEN_SGROUP, UTOKEN_SUSER, and UTOKEN_SNODE fields.

VOLSER, VOLUME

Volume serial. This field is found in most data set and volume-related records (SMF record types 14, 15, 17, 18, 19, 21, 36, 42, 60, 62, 64 and 69), HSM function statistics records, RACF processing records (SMF record types 80 and 83) for class=DATASET, ACF2 data set use records, and TSS processing records (SMF record type 80) for class=DATASET.

Note: VOLSER is a repeated field. In the current version of Security zSecure, this repeated field may contain duplicate volume serials for some record types.

VOLSER_OR_SMS

Volume serial or, if the volume is SMS-managed, *SMS*. This field is found in most data set and volume-related records (SMF record types 14, 15, 17, 18, 19, 21, 36, 60, 62, 64 and 69), HSM function statistics records, RACF processing records (SMF record types 80 and 83) for class=DATASET, ACF2 data set use records, and TSS processing records (SMF record type 80) for class=DATASET.

Note: VOLSER_OR_SMS is a repeated field. In the current version of Security zSecure, this repeated field may contain duplicate volume serials for some record types.

VTAMNET_IS_REMOTE

VTAMNET_IS_REMOTE is a flag field that indicates whether the VTAM network ID associated with a CICS transaction is from a remote network. The value is TRUE if it is remote. If the VTAM net ID information is not available, this field is not reported.This field is supported on CICS monitoring subrecords.

VTAMNETID

For CICS monitoring performance sub records, this field returns the name by which the network unit-of-work ID is known within the originating system. This name is assigned at transaction attach time using either a STCK-derived token created by the originating system, or the network unit-of-work ID passed as part of an IRC (MRO) or ISC (APPC) attach function management header (FMH).

WEEKDAY

Day of the week the record was written. For SELECT/EXCLUDE processing, either specify the weekday name in full or use the first three characters of the weekday name (for example, SUNDAY or SUN for Sunday). The default output is also three characters long; specify an overriding output length of 9 characters to output the full weekday. This field is found in all SMF record types. For SELECT/EXCLUDE processing, a range of weekdays separated by a colon (:) is allowed, as indicated in the following examples. A range of MON:WED is inclusive, for example, Monday, Tuesday, and Wednesday. For use with the relational operators <, <=, >, and >=, the sort order has been defined as Sunday < Monday < ... < Saturday.

```
SELECT WEEKDAY=MON                      /* One day */
SELECT WEEKDAY=(MON, FRI)               /* Two days */
SELECT WEEKDAY>=TUE WEEKDAY<=SAT        /* Day range */
```

```
SELECT WEEKDAY=TUE:SAT                    /* Day range */
SELECT WEEKDAY>=FRI OR WEEKDAY<=MON       /* Day range */
SELECT WEEKDAY=FRI:MON                    /* Day range */
```

YEAR

Year the record was written. For SELECT/EXCLUDE processing, a YEAR value in the range 0 to 99 is only allowed if you suppress message CKR051I and then implies a year the 20th century. For example, YEAR=94 is equal to YEAR=1994. This field is found in all SMF record types. For SELECT/EXCLUDE processing, a range of years separated by a colon (:) is allowed, as indicated in the following examples.

```
SELECT YEAR=1994                          /* One year */
SELECT YEAR=(1994, 1988, 1989)            /* Three years */
SELECT YEAR>=1992 YEAR<=1996              /* Year range */
SELECT YEAR=1992:1996                     /* Year range */
```

Tables of fields and record types

SMF records contain various types of event information depending on the source of the events. For information on the fields that apply to different types of SMF records, see the following topics:

Fields common to all record types

Most fields are only found in the predefined SMF record types; the following list includes the common fields found in all record types. The following table documents the fields common to all record types.

Fields common to all SMF record types

DATE
FIELDVAL
MONTH
MONTHDAY
RECNO
RECORDDESC
RECORDLENGTH
SMFDD
SUBTYPE
SYSTEM
SYSTYPE
TIME
TYPE
WEEKDAY
YEAR

Note: The SUBTYPE field is found in all records that support subtypes. This field is defined in the SMF record header.

Supported record types

Table 533 on page 1389 shows all record types with a short description of their content. It also shows whether this stock description is the only thing present in the RECORDDESC field (`Stock=Y`) or if it contains more data. The details column indicates whether there are more fields present than just the common fields. See "Record types vs. field names" on page 1391 for an exact list of extra fields.

Table 533. SMF records - supported record types

SMF record type	Description	Details	RECORDDESC field only provides stock description (Y) or contains additional information (N)
0	IPL		Y
2	Dump Header		Y
3	Dump Trailer		Y
4	Step Termination	Y	Y
5	Job Termination	Y	Y
6	Output Writer or PSF	Y	Y
7	Data Lost		
8	I/O Configuration		Y
9	VARY Device ONLINE		
10	Allocation Recovery	Y	Y
11	VARY Device OFFLINE		
14	INPUT or RDBACK Data Set Activity	Y	
15	OUTPUT, UPDATE, INOUT, or OUTIN Data Set Activity	Y	
16	DFSORT Statistics	Y	Y
17	Scratch Data Set Status	Y	
18	Rename Data Set Status	Y	
19	Direct Access Volume	Y	Y
20	Job Initiation	Y	
21	Error Statistics by Volume	Y	
22	Configuration		Y
23	SMF Status		Y
24	JES2 Spool Offload	Y	Y
25	JES3 Device Allocation	Y	Y
26	JES2 or JES3 Job Purge	Y	
28	NPM Statistics		Y
30	Common Address Space Work	Y	
31	TIOC Initialization		Y
32	TSO/E User Work Accounting	Y	
33	APPC/MVS TP Accounting	Y	
34	TS-Step Termination	Y	
35	LOGOFF	Y	
36	ICF Catalog	Y	Y
37	Netview Hardware Monitor		Y
39	Netview (NLDM) Response Time		Y

14. HSM Daily/Volume Statistics: The SMF record number of this record type is installation-dependent.
15. Record type 81 is supported through defined variables in CARLa member CKAS0081.
16. Record type 89 is supported through defined variables in CARLa member CKAS0089.
17. Record type 90 is supported through defined variables in CARLa member CKAS0090.
18. HSM function statistics: The SMF record number of this record type is installation-dependent.
19. ACF2: The SMF record number of this record type is installation-dependent, default is 230.

Table 533. SMF records - supported record types (continued)

SMF record type	Description	Details	RECORDDESC field only provides stock description (Y) or contains additional information (N)
40	Dynamic DD	Y	Y
41	DIV ACCESS/UNACCESS	Y	Y
42	DFSMS Statistics and Configuration		Y
43	JES2 or JES3 Start		Y
45	JES2 Withdrawal or JES3 Stop		Y
47	JES2 or JES3 SIGNON/Start Line/LOGON		Y
48	JES2 or JES3 SIGNOFF/Stop Line/LOGOFF		Y
49	JES2 or JES3 Integrity		Y
50	ACF/VTAM Tuning Statistics		Y
52	JES2 LOGON/Start Line		Y
53	JES2 LOGOFF/Stop Line		Y
54	JES2 Integrity		Y
55	JES2 Network SIGNON		Y
56	JES2 Network Integrity		Y
57	JES2 or JES3 Network Transmission		Y
58	JES2 Network SIGNOFF		Y
59	MVS/BDT File-to-File Transmission		Y
60	VSAM Volume Data Set Updated	Y	
61	ICF Define Activity	Y	
62	VSAM Component or Cluster Opened	Y	
63	VSAM Catalog Entry Defined	Y	Y
64	VSAM Component or Cluster Status	Y	
65	ICF Delete Activity	Y	
66	ICF Alter Activity	Y	
67	VSAM Catalog Entry Delete	Y	Y
68	VSAM Catalog Entry Renamed	Y	Y
69	VSAM Data Space Defined, Extended, or Deleted	Y	Y
70	RMF CPU Activity		Y
71	RMF Paging Activity		Y
72	RMF Workload Activity and Storage Data		Y
73	RMF Channel Path Activity		Y
74	RMF Device and XCF Activity		Y
75	RMF Page/Swap Data Set Activity		Y
76	RMF Trace Activity		Y
77	RMF Enqueue Activity		Y

Table 533. SMF records - supported record types (continued)

SMF record type	Description	Details	RECORDDESC field only provides stock description (Y) or contains additional information (N)
78	RMF Monitor I Activity		Y
79	RMF Monitor II Activity		Y
80	RACF Processing/TSS Audit	Y	
81	RACF Initialization[15]		Y
82	ICSF Integrated Cryptographic Facility		Y
83	Security Events	Y	
84	JES3 Monitoring Facility (JMF) Data		Y
85	OAM Object Access Method		Y
88	System Logger Data		Y
89	Product Usage Data[16]		
90	System Status[17]		
91	Batch Pipes/MVS Statistics		Y
92	OpenMVS File System activity	Y	
94	IBM Tape Library Dataserver Statistics		Y
96	The Integrated Reasoning Shell TIRS Statistics		Y
97	Foreign Enclave Resource Data from *list of systems*		
99	SRM System Resource Manager decision		Y
100	DB2 Statistics		Y
101	DB2 Accounting		Y
102	DB2 performance and audit		
103	IBM HTTP Server		Y
108	Domino® Server Statistics		Y
109	z/OS Firewall Technologies	Y	
110	CICS/ESA Statistics		Y
115	MQSeries Statistics		Y
116	MQSeries Accounting Information		Y
118	TCP/IP Telnet and FTP	Y	
119	Connectivity Statistics	Y	
120	Websphere AS Performance Statistics		Y
HSM Daily/ Volume Statistics	DFHSM Daily or Volume Statistics[14]	Y	Y
HSM function statistics	DFHSM Function Statistics[18]	Y	Y
ACF2	ACF2 all events[19]	Y	Y

Record types vs. field names

This section lists the predefined SMF record types and the fields found in those records. The list includes only those record types have fields other than the

common and RECORDDESC fields, and only those fields limited to some SMF record types. The fields that are only found in RACF or ACF2 processing records are not included; see the next tables for the fields available in RACF and ACF2 records.[20]

For the list of fields organized by SMF record types, see the following topics:

- Table 534 on page 1393 for SMF record types 1- 26
- Table 535 on page 1394 for SMF record types 30 - 65
- Table 536 on page 1395 for SMF record types 66 - 119

20. HSM Func Stats: The SMF record number of this record type is installation-dependent.

Table 534. Predefined SMF record types: fields available by type - SMF records 1-26

	4	5	6	10	14	15	16	17	18	19	20	21	24	25	26
ACTION															
CATALOG															
CLASS					•	•		•	•						
COMPCODE	•	•													
COMPSTAT	•	•													
DATASET					•	•		•	•				•		
DSN															
DSTIP															
DSTPORT															
EXPLANATION															
FILE					•	•									
GROUP					•	•	•	•	•		•				
HOSTNAME															
INTENT					•	•		•	•						
JOBCLASS		•													•
JOBELAPSED		•													
JOBID					•	•		•	•		•				•
JOBNAME	•	•	•	•	•	•	•	•	•		•		•	•	•
JOBTAG	•	•	•	•	•	•	•	•	•		•			•	•
LOGSTR															
MEMBER															
MEMBER_ALIAS			•												
MEMBER_OLDNAME			•												
MSGID															
NAME		•									•				•
PRIORITY															
PROCNAME															
PROFILE					•	•		•	•						
PROGRAM	•														
QUAL					•	•		•	•						
RESOURCE					•	•		•	•						
SMFUSER	•	•	•	•	•	•		•	•		•				•
SRCIP															
SRCPORT															
STEPNAME	•														
SUBTYPE													•		
TERMINAL					•	•		•	•		•				
TSOCMD															
TSOCMDCNT															
UNITTYPE					•	•									
UNIX _ACCESS _ALLOWED															
UNIX_ACCESS _FILENAME															
UNIX _ACCESS _INTENT															
UNIX _ACCESS _PATHNAME															
UNIX_FILENAME															
UNIX _FILETYPE															
UNIX _FUNCTION															
UNIX _PATHNAME															
USER					•	•	•	•	•		•				
VOLSER					•	•		•	•	•		•			
VOLSER _OR_SMS					•	•		•	•	•		•			

Table 534. Predefined SMF record types: fields available by type - SMF records 1-26 (continued)

	4	5	6	10	14	15	16	17	18	19	20	21	24	25	26

Table 535. Predefined SMF record types: fields available by type - record types 30-65

	30	32	33	34	35	36	40	41	42	60	61	62	63	64	65
ACTION									•						
APPL															
CATALOG						•					•	•	•	•	•
APPL															
CLASS									•	•	•	•		•	•
COMPCODE	•														
COMPSTAT	•														
DATASET									•	•	•	•	•	•	•
DSN															
DSTIP															
DSTPORT															
EXPLANATION															
FILE														•	
GROUP	•	•	•						•	•	•	•		•	•
HOSTNAME															
INTENT									•		•			•	•
JOBCLASS	•														
JOBELAPSED	•														
JOBID	•	•								•	•	•		•	•
JOBNAME	•	•	•	•	•	•	•	•		•	•	•	•	•	•
JOBTAG	•	•	•							•	•	•	•	•	•
LOGSTR															
MEMBER									•						
MEMBER_ALIAS									•						
MEMBER_OLDNAME									•						
MSGID															
NAME	•	•													
PRIORITY															
PROCNAME	•														
PROFILE									•	•	•	•		•	•
PROGRAM	•	•		•		•									
QUAL									•	•	•	•		•	•
RESOURCE									•	•	•	•		•	•
SMFUSER	•	•		•	•	•	•			•	•	•	•	•	•
SRCHOST									•						
SRCIP									•						
SRCPORT															
STEPNAME	•	•	•	•											
SUBTYPE	•	•	•					•							
TERMINAL	•	•								•	•	•		•	•
TSOCMD		•													
TSOCMDCNT		•													
UNITTYPE	•										•	•		•	•
UNIX _ACCESS _ALLOWED															
UNIX_ACCESS _FILENAME															
UNIX _ACCESS _INTENT									•						
UNIX _ACCESS _PATHNAME															
UNIX_FILENAME									•						
UNIX _FILETYPE									•						

Table 535. Predefined SMF record types: fields available by type - record types 30-65 (continued)

UNIX _FUNCTION									•						
UNIX _PATHNAME									•						
USER	•	•	•						•	•	•	•		•	•
VOLSER						•			•	•		•		•	
VOLSER _OR_SMS						•				•		•		•	
	30	32	33	34	35	36	40	41	42	60	61	62	63	64	65

Table 536. Predefined SMF record types: fields available by record types 66-119, HSM Functions, and ACF2

	66	67	68	69	80	83	86	92	102	109	110	118	119	HSM Func Stats	ACF2
ACTION															
APPL						•					•				
CATALOG	•	•	•	•											
CSSMTP_ CKPFILE													•		
CSSMTP_BADSPOOLDISP													•		
CSSMTP_CN_ESMTP													•		
CSSMTP_CN_FIPS140													•		
CSSMTP_CN_LOCAL_IP													•		
CSSMTP_CN_LOCAL_PORT													•		
CSSMTP_CN_REMOTE_IP													•		
CSSMTP_CN_REMOTE_PORT													•		
CSSMTP_CN_TLS_SSL_PROTO													•		
CSSMTP_CN_TLSNC													•		
CSSMTP_CONFIG_FILE CSSMTP_DATETIME													•		
CSSMTP_DEAD_LETTER_ACTN													•		
CSSMTP_DEAD_LETTER_DIR															
CSSMTP_DOMAIN_NAME													•		
CSSMTP_EXTWRTNAME													•		
CSSMTP_HOSTNAME													•		
CSSMTP_LOGFILE													•		
CSSMTP_LOGLEVEL													•		
CSSMTP_MAIL_ADMIN_MBOX													•		
CSSMTP_MH_CMD_ERROR													•		
CSSMTP_MH_DATE													•		
CSSMTP_MH_FROM													•		
CSSMTP_MH_MSGID													•		
CSSMTP_MH_RCPT_REPLY													•		
CSSMTP_MH_REPLY_TO_ERROR													•		
CSSMTP_MH_SUBJECT													•		
CSSMTP_MH_TO													•		
CSSMTP_REPORT													•		
CSSMTP_RTN_TO_MAIL_FROM													•		
CSSMTP_SI_SYSTEM													•		
CSSMTP_SMF119													•		
CSSMTP_ST_CN_RCVD_CNT													•		
CSSMTP_STACK													•		
CSSMTP_TS_DSTIP													•		
CSSMTP_TS_NAME													•		
CSSMTP_TS_PORT													•		
CSSMTP_TS_SECURE													•		
CSSMTP_TS_TYPE													•		
CSSMTP_USEID															
CSSMTP_USEREXIT															
CLASS	•				•	•	•							•	•
COMPCODE												•			
COMPSTAT															

Table 536. Predefined SMF record types: fields available by record types 66-119, HSM Functions, and ACF2 (continued)

DATASET	•	•	•		•	•						•		•	•
DSN												•	•		
DSTIP										•		•	•		
DSTPORT										•		•	•		
EXPLANATION										•					
FILE															•
GROUP	•				•	•		•						•	•
HOSTNAME										•		•	•		
INTENT	•				•	•									
JOBCLASS															
JOBELAPSED															
JOBID	•				•	•		•			•				•
JOBNAME	•	•	•	•	•	•		•			•			•	•
JOBTAG	•	•	•	•	•	•		•						•	•
LOGSTR					•	•									•
MEMBER													•		
MEMBER_ALIAS															
MEMBER_OLDNAME															
MSGID										•					
NAME					•	•									•
PRIORITY										•					
PROCNAME															
PRODUCT						•					•				
PRODUCT_FMID						•					•				
PROFILE	•				•	•								•	
PROGRAM						•									•
QUAL	•				•	•								•	
RACF_LINK_AUDIT						•									
RACF_LINK_EVENT						•									
RESOURCE	•				•	•								•	
RLOG_DATA						•									
SECURITY_EVENT								•							
SMFUSER	•	•	•	•	•	•									•
SRCIP						•				•	•	•	•		
SRCPORT						•				•		•	•		
STEPNAME								•							•
SUBTYPE						•					•				
TERMINAL	•				•	•		•							
TSOCMD															
TSOCMDCNT															
UNITTYPE	•														
UNIX _ACCESS _ALLOWED					•										
UNIX_ACCESS _FILENAME					•	•									•
UNIX _ACCESS _INTENT					•										•
UNIX _ACCESS _PATHNAME					•	•									•
UNIX_FILENAME					•	•		•				•	•		•
UNIX _FILETYPE					•			•							
UNIX _FUNCTION					•										•
UNIX _PATHNAME					•			•				•	•		•
USER	•				•	•		•		•		•	•	•	•
VOLSER				•	•	•								•	•

Table 536. Predefined SMF record types: fields available by record types 66-119, HSM Functions, and ACF2 (continued)

VOLSER _OR_SMS				•	•	•									•
	66	67	68	69	80	83	86	92	102	109	110	118	119	HSM Func Stats	ACF2

Fields found only in CICS records

zSecure can report on information contained in SMF audit trail records related to the CICS monitoring performance subrecords (SMF record type 110, subtype 1, subclass 3)

Table 537 lists the fields that contain the information extracted from the CICS monitoring performance records. These records do not include the common fields found in all record types. For information on those fields, see "Fields common to all record types" on page 1388.

Table 537. CICS monitoring records

Field	Field description available at ...
CICS_MONITOR_CLASS	1278
CICS_PERFORMANCE_DATA	1279
CICS_SPECIFIC_APPL	1279
CICS_TERM	1279
CICS_TTYPE	1279
ELAPSED	1290
EVENT_DATETIME	1305
SUBRECORD	1350
SUBRECORDNO	1351
TRANSACTION	1373
VTAMNET_IS_REMOTE	1386
VTAMNETID	1386

Fields found only in CSSMTP records

zSecure can report on information contained in SMF type 119, subtype 48-52 records produced by the Communications Server SMTP client (CSSMTP). Information from the following kinds of records can be shown:

- CSSMTP configuration records (SMF record type 119, subtype 48)
- CSSMTP connection records (SMF record type 119, subtype 49)
- CSSMTP mail records (SMF record type 119, subtype 50)
- CSSMTP spool records (SMF record type 119, subtype 51)
- CSSMTP statistics records (SMF record type 119, subtype 52)

The CARLa fields associated with these records are described in "SMF: SMF records" on page 1276. Most of these fields are only found in CSSMTP SMF records. The name of each field begins with the character string `CSSMTP`.

Fields found only in DB2 records

zSecure can report on information contained in SMF audit trail records related to the following DB2 record types:

- DB2 Statistics records (SMF record type 100)

- DB2 Accounting records (SMF record type 101)
- DB2 Performance records (SMF record type 102)

Table 538 lists the fields that contain the information extracted from the DB2 audit records. These records do not include the common fields found in all record types that are described earlier. (See "Fields common to all record types" on page 1388.)

Table 538. DB2 SMF records - field descriptions

Field	Field description available at ...
DB2_APPL_USERID	1286
DB2_AUTHID	1286
DB2_COMMAND	1287
DB2_CONNECTION	1287
DB2_CONTEXT	1287
DB2_ENDUSER_USERID	1288
DB2_OBJECT	1288
DB2_OBJECT_TYPE	1288
DB2_ORIGINAL_OPERATOR	1288
DB2_PLAN	1288
DB2_ROLE	1288
DB2_SECAUTHID	1289
DB2_SQLID	1289

Fields found only in IP stack configuration records

The fields found only in the SMF records for TCP/IP configuration information are listed in the SMF field description chapter. These fields begin with the character string IP.

The TCP/IP configuration record types, common fields, and field descriptions are also documented in the IP newlists in "IP: Profile information for TCP/IP configuration" on page 1054. In the IP NEWLIST field descriptions, the fields are the same as the SMF fields, but they have different names. The IP NEWLIST field names are not preceded by the IP configuration information type. For example, the SMF field for IP_RULE_SRCPRT is equivalent to the SRCPRT field in the IP_RULE NEWLIST.

Fields found only in Omegamon security audit records

zSecure can report on information contained in SMF audit trail records related to Omegamon commands. These records are generated from Omegamon Classic address spaces (z/OS, DB/2, IMS, CICS) that have been configured for auditing. Table 539 on page 1399 lists the fields that contain the information extracted from the Omegamon audit records.

The common fields found in all record types, and the fields that are found in one or more record types other than RACF processing records (except for the R_auditx records), are not included in this table. See "Fields common to all record types" on page 1388 and see the previous tables. The following fields contain the information extracted from these records.

Table 539. Omegamon audit records - field descriptions

Field	Field description available at ...
OMCMD_NAME	1336.
OMCMD_ALLOWED	1336.
OMCMD_TEXT	1336.
OMCMD_TYPE	1336.

You can also generate pre-defined reports for Omegamon auditing records from the Events menu (EV.6). For more information, see "Reporting on Omegamon events (EV.6)" on page 572.

Fields for User Security Token

The following fields for User Security Token information are documented in the SMF section. These fields document the contents of the security token and information regarding the Port of Entry. These fields apply to the following record types: RACF processing records (SMF record types 80 and 83 subtype 1), DB2 subtypes (SMF record type 102), and CSSMTP client records (SMF record type 119) with subtype 48.

- "UTOKEN" on page 1381
- "UTOKEN_POE" on page 1383
- "UTOKEN_POECLASS" on page 1383
- "UTOKEN_POE_NETWORK" on page 1384
- "UTOKEN_SESSION" on page 1384
- "UTOKEN_SGROUP" on page 1385
- "UTOKEN_SNODE" on page 1385
- "UTOKEN_SUSER" on page 1385
- "UTOKEN_XNODE" on page 1385

Fields found in RACF processing records

The following table lists the fields that are found in RACF processing records (SMF record types 80 and 83 subtype 1). The 'common' fields found in all record types, and the fields that are found in one or more record types other than RACF processing records (except for the R_auditx records), are not included in this table. See the other tables.

Table 540. SMF RACF processing records - field descriptions

Field name	Meaning	Event types
ACCESS	Allowed access	ACCESS
APPL	Application name	RACINIT ACCESS
DESCRIPTOR	Record descriptor	all
EVENT	Event code	all
EVENTDESC	Description of event	all
EVENTQUAL	Event qualifier code	all
KERB_NAME	Kerberos principal name	all
KERB_SOURCE	Kerberos login request source	all
KERB_STATUS	Kerberos KDC status code.	all

Table 540. SMF RACF processing records - field descriptions (continued)

Field name	Meaning	Event types
LOGSTR	Log string	ALLSVC GENERAL
OWNER	Profile owner	all
PKCS11_TOKEN	Token name	RACDCERT
RACFAUTH	RACF authority used	all
RACFCMD	RACF command string	ALLCOMMAND
RACFCMD_AUTH	Authority specified in a RACF command	ADDUSER ALTUSER CONNECT
RACFCMD_GROUP	Target group of RACF command	ADDGROUP ALTGROUP CONNECT DELGROUP PERMIT REMOVE
RACFCMD_KEYWORDS	Keywords used in a RACF command	ALLCOMMAND
RACFCMD_KEYWORDS_EFF	Effective keywords used in a RACF command	ALLCOMMAND
RACFCMD_OWNER	New owner specified in a RACF command	ADDGROUP ADDSD, ADDUSER ALTDSD ALTGROUP , ALTUSER CONNECT RALTER RDEFINE REMOVE
RACF_SECTION	User-defined fields	all
RACFCMD_USER	Target user of RACF command	ADDUSER ALTUSER CONNECT DELUSER PASSWORD PERMIT REMOVE
REASON	Reason to log the event	all
RELOCATE	List of relocate section codes	all
RTOKEN	Resource security token	ACCESS
RTOKEN_FLAGS	Flags from resource security token	ACCESS
SECLABEL	User's security label	ACCESS
UNIX_ACCESS_ALLOWED	Access allowed	UNIX-related
UNIX_ACCESS_INTENT	Access intent	UNIX-related
UNIX_ACCESS_ORIGIN	Access origin	UNIX-related
UNIX_ACCESS_USED	Access used	UNIX-related
UNIX_FILENAME	File name	UNIX-related
UNIX_FUNCTION	Audit function code	UNIX-related
UTOKEN	User's security token	all

Table 540. SMF RACF processing records - field descriptions (continued)

Field name	Meaning	Event types
UTOKEN_FLAGS	Flags from user security token	all
UTOKEN_POE	Port-Of-Entry	all
UTOKEN_POECLASS	Port-Of-Entry class	all
UTOKEN_POE_NETWORK	Port Of Entry network	all
UTOKEN_SESSION	Session type	all
UTOKEN_SGROUP	Connect group of submitting user	all
UTOKEN_SNODE	Submitting node	all
UTOKEN_SUSER	Submitting user	all
UTOKEN_XNODE	Execution node	all

Fields found in R_auditx records

The R_auditx service is used to create audit records for Enterprise and Identity Mapping (EIM), subtype 2 events.

The following table lists the fields that are found in these records. The common fields found in all record types are not included in this table. (See "Fields common to all record types" on page 1388.)

Table 541. SMF R_auditx records - Fields found in Enterprise Identity Mapping (EIM) Event 2

Field name	Applications
APPL	All
CERTIFICATE_ISSUER	All
CERTIFICATE_SUBJECT	All
CLASS	All
DESCRIPTOR	All
DSTIP	EIM
DSTPORT	EIM
EVENT	All
EVENTDESC	All
EVENTQUAL	All
GROUP	All
JOBID	All
JOBNAME	All
JOBTAG	All
LOGSTR	All
PROFILE	All
RACFAUTH	All
REASON	All
RELOCATE	All
RESOURCE	All
SECLABEL	All

Table 541. SMF R_auditx records - Fields found in Enterprise Identity Mapping (EIM) Event 2 (continued)

Field name	Applications
SMFUSERID	All
TERMINAL	All
USER	All

Fields found only in security audit records (SMF record 83, subtype 4, 5 and 6)

Table 542 lists the fields that are only found in security audit records generated by the following applications:

- IBM Tivoli Key Lifecycle Manager (SMF record type 83, subtype 6)
- IBM Websphere Application Server, version 7.0 and later (SMF record type 83, subtype 5)
- Linux events logged remotely by the Linux audispd plug-in (daemon) or .JZOS toolkit

This information does not include common fields found in all record types or the fields that are found in one or more record types other than the audit security records. See "Fields common to all record types" on page 1388 and Table 534 on page 1393.

Table 542. SMF record types - fields only found in security audit records (SMF record type 83, subtype 5 and 6)

Field name	Meaning	Record subtype
R_ACCESS	Allowed access	5- Websphere Application Server events
R_ACTION	Action type	ACCESS events
R_EVENT	Event type	6- Tivoli Key Lifecycle Manager events Websphere Application Server events
R_INTENT	Intended access	6- Tivoli Key Lifecycle Manager events Websphere Application Server events
RACF_LINK_AUDIT	Serial number for the Linux Audit record which is shared by all records created from the same event.	4 - zLinux events
RACF_LINK_EVENT	Serial number for a security audit event from a zLinux system.	4 - zLinux events
R_LOGDATA	Application-specific data for the event including all field names and values in a `fieldname=value` format.	4 - zLinux events
R_LOGRECORD	Native java log record	6 - Tivoli Key Lifecycle Manager events
R_MGMT_ATTR	Information about objects involved in operation	5 - Websphere Application Server events

Table 542. SMF record types - fields only found in security audit records (SMF record type 83, subtype 5 and 6) (continued)

Field name	Meaning	Record subtype
R_MGMT_CMD	Command performed	5 - Websphere Application Server events
R_MGMT_TYPE	Management operation type	5 - Websphere Application Server events
R_RESOURCE	Resource name in application context	5 - Tivoli Key Lifecycle Manager events Websphere Application Server events
R_RESULT	Event outcome	5 - Websphere Application Server events
R_ROLECHECK	Role checked	5 - Websphere Application Server events
R_ROLEGRANT	Role granted	5 - Websphere Application Server events
R_USER	User ID used for authentication or authorization	6 - Tivoli Key Lifecycle Manager events Websphere Application Server events
SRCHOST	Port number of remote host	5 - Websphere Application Server events

SMFOPT: SMF Subsystems

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The SMFOPT NEWLIST (NEWLIST TYPE=SMFOPT) provides information about the SMF subsystem in a MVS system. This NEWLIST generates one entry per SMF subsystem in an MVS system. Each entry is uniquely identified by the fields SYSTEM SUBSYS.

Field descriptions

The SMFOPT NEWLIST provides the following fields for reporting.

ACTIVE

For any SMF record type, this flag field indicates if the SMF record type is recorded for this SMF subsystem. This field is repeated and can be combined with the RECORD and DESC fields.

ACTREC, WRTREC

A repeat group giving a list of all active record types. Any active record type has ACTIVE=YES.

Note: When this field is combined with the ACTIVE or DESC fields, the entries do not line up correctly.

AUDITCONCERN

This field indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs because the content might change. The

AUDITCONCERN field can contain one or more concerns separated by commas. The following audit concerns have currently been defined:

- RACF records suppressed

  RACF is active, and SMF record types 80 or 81 (or 83 if MLACTIVE is set) are suppressed for the subsystem. As a result, no RACF processing or status records are available. System system security events cannot be audited.

- Job start not recorded

  Job start records (SMF record type 20 and type 30, subtype 1) are suppressed. As a result, job starts cannot be audited. Note that RACF does *not* log job start events unless a security-related event occurred.

- Data loss not recorded

  SMF records can be lost in the system (the system-wide options NOBUFFSHALT and LASTDSHALT are not both set), and the subsystem does not record SMF type 7 (Data lost). If a data loss should occur, this is not logged; an auditor is not able to tell when SMF data were lost.

- Data set activity not recorded

  One or more types of data set activity records (record types 14-15, 17-18, 60-62, 64-67) are suppressed. Security zSecure is not able to analyze all data set activities.

- Interval recording not active

  Step interval records (SMF record type 30, subtypes 2 and 3) are not written for the subsystem. Accounting information for long-running jobs are lost if the system unexpectedly goes down.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 543. SMFOPT NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

DESC, DESCRIPTION

A string of up to 64 characters giving, for any SMF record type, a short description of the record type and subtype. This field is repeated and can be combined with the RECORD and ACTIVE fields.

DETAIL

A flag indicating whether detail recording is active. When detail recording is active (DETAIL=YES), SMF record types 30 and 32 contain additional information such as total CPU time used and EXCP counts for started tasks. If detail recording is inactive (DETAIL=NO), SMF record type 30 contains EXCP counts for TSO/E users and batch jobs only.

EXITCNT, EXITCOUNT

Number of SMF exits active for this subsystem. The exits can be listed with the ADDRESS and PROGRAM fields, or with NEWLIST TYPE=EXIT.

INACTREC, SUPREC

A repeat group giving a list of all inactive (suppressed) record types. Any inactive record type has ACTIVE=NO.

Note: When this field is combined with the ACTIVE or DESC fields, the entries do not line up correctly.

INTERVAL

The SMF recording interval in the format HH:MM:SS. If this value is blank, no interval records are written; any other value specifies the length of the interval in hours, minutes and seconds. At the end of each interval, SMF record types 30 and 32 are written to record accounting data for the past interval.

This field is output-only: it cannot be used in the SELECT and EXCLUDE commands.

PARTCNT, PARTCOUNT

The number of different SMF record types partially written, for example some subtypes are written, and some subtypes are suppressed.

PROGRAM

Indicates, for each exit, the program name of the exit as present in the in-storage SMF control blocks. This field is repeated and can be combined with the ADDRESS field. More information about the exit routine can be displayed with NEWLIST TYPE=EXIT (select APPL=SMF).

RECORD, REC

The type and subtype of an SMF record, in the format '**type**' or '**type-subtype**'. This field is repeated and can be combined with the ACTIVE and DESC fields.

SUBSYS

Name of the subsystem for which the SMF options are set. This name, when combined with the SYSTEM field, identifies an entry in this NEWLIST type.

The subsystem name can be SYS (for system-wide settings), one of the SMF-defined types STC and TSO, or an actual subsystem such as JES2. The NEWLIST TYPE=SUBSYS can be used to report on actual subsystems.

SUMMARY

A single line summarizing the SMF recording options, in the format `suppress n n:n n(s,s)`, `write n n:n n(s,s)` (with `n` record types, `s` record

subtypes, suppress none, write none, write all, or suppress all The suppress and write lines are both generated, and the shortest is taken.

SUPCNT, SUPCOUNT

The number of different SMF record types suppressed. Any record type that is suppressed has ACTIVE=NO.

SYSTEM

The name of the system. This is the SMF system ID. This name, when combined with the SUBSYS field, identifies an entry in this NEWLIST type. The field length is 8 characters to cater to VM systems.

WRTCNT, WRTCOUNT

The number of different SMF record types written. Any record type written has ACTIVE=YES.

SPT: RACF Started Procedure Table

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•		

The SPT NEWLIST (NEWLIST TYPE=SPT) provides information about the Started Procedure Table (SPT). It generates one entry per table entry per system. A unique key is SYSTEM ORDER. Unless otherwise stated, all fields can be used for SELECT and EXCLUDE processing as well as in the following output commands: LIST, SORTLIST, DISPLAY and SUMMARY.

The Started Procedure Table is loaded at IPL from module ICHRIN03. Inconsistencies in this table can be identified by running VERIFY STC.

Field descriptions

The SPT NEWLIST provides the following fields for reporting.

ATTR, AUTH

A string containing the started procedure attributes. If PRIVILEGED=YES, this field is set to *Privileged*. If TRUSTED=YES, this field is set to *Trusted*. Otherwise, the field is empty.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The value is taken from the ALLOC COMPLEX parameter or default to a system name.

GROUP

The RACF group ID assigned to this started procedure. If this field is empty, no specific group ID has been assigned. In that case, the started task runs under the default group of the selected user ID.

ORDER, ORG

The original order (entry number) of this started procedure in the started procedure table. The first entry in the table has ORDER=1.

PRIVILEGED

Flag field that indicates in a RACF system that the started procedure runs with the privileged attribute. All access requests–except those that request a profile to be returned in-storage through the use of the CSA or PRIVATE keywords–are granted and auditing is suppressed. If the PRIVILEGED flag is set, RACF ignores the value of the TRUSTED setting. Accordingly, the SPT NEWLIST, also reports that the TRUSTED flag as not set.

PROCNAME

The name of the started procedure. When combined with the SYSTEM field, this field identifies an entry in this NEWLIST type.

The last entry in the table can contain an asterisk (*) to indicate a generic entry. Actual procedures matching this entry can be displayed by running VERIFY STC.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system ID. The field length is 8 characters to cater to VM systems. When combined with the PROCNAME field, this field identifies an entry in this NEWLIST.

TRUSTED

Flag field that indicates that the started procedure in a RACF system runs with the trusted attribute. Most access request are granted and only limited auditing possibilities exist. Access requests that request a profile to be returned in-storage through the use of the CSA or PRIVATE keywords are not authorized. Auditing is only possible using SETROPTS LOGOPTIONS and the UAUDIT setting for the user ID. If the PRIVILEGED flag is set, RACF ignores the value of the TRUSTED setting. Accordingly, SPT NEWLIST TYPE, also reports the TRUSTED flag as not set.

USER, USERID

The RACF user ID assigned to this started procedure. If this field is empty, no specific user ID has been assigned, which means that the started procedure runs under the generic entry, PROCNAME=*.

SUBSYS: MVS Subsystems

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The SUBSYS NEWLIST (NEWLIST TYPE=SUBSYS) describes the MVS subsystems. Each entry can be uniquely identified by either SYSTEM NAME or SYSTEM ORG.

Field descriptions

The SUBSYS NEWLIST provides the following fields for reporting.

ARDR

Flag field that describes the ARDR flag, which indicates if the subsystem supports the allocation of a special internal reader.

AUDITCONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs because the contents can change. This field can contain any of the following audit concerns.

- **Control block in user-key common storage**

  Either the SSCT or the SSVT lies in writable common storage making it possible for any user to change the subsystem. If the SSCT is writable, immediate action is required. If the SSVT is writable, the subsystem must be reviewed to see whether the SSVT is actually used.

- **Function in user-key common storage**

  A subsystem function lies in writable common storage making it possible for any user to change the function code to subvert the subsystem. If the subsystem function runs authorized, the change can potentially subvert the whole MVS system. Immediate action is required.

- **User pointer in user-key common storage**

  The SUSE or SUS2 user pointer seems to point to writable common storage. The subsystem must be reviewed. First, check whether the SUSE and SUS2 pointers are actually used. If random user data is used, then this is a false alarm. Second, check the use of the writable data. If the subsystem does not use the areas, no immediate action is required. However, the supplier of the subsystem should not use user-writable common storage. If the subsystem uses the area as a vector table, this audit concern is serious.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 544. SUBSYS NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can be taken from the `ALLOC COMPLEX` parameter or default to a system name.

DESCRIPTION

Text field that contains a description of the subsystem, if it is known to zSecure. The value is the name of the package that normally creates this subsystem. Do not rely on the exact value of this field in your programs because the contents can change.

FIB

Flag field that indicates whether serialization of Foreground Initiated Background (FIB) requests is required. For example, TSO provides the FIB commands SUBMIT, CANCEL, and STATUS.

FUNCTION

This repeated field contains the documented description of a subsystem function. It is part of the structured repeat group described with FUNCTION_NO.

Note: The FUNCTION field is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_ADDRESS

This repeated field contains the address of a subsystem function. It is part of the structured repeat group described with FUNCTION_NO.

Note: Only available if the SSVT_ADDRESS field is not zero.

FUNCTION_AMODE

This repeated field contains the addressing mode of a subsystem function. It is part of the structured repeat group described with FUNCTION_NO. The value can be *24* or *31*.

FUNCTION_AT

This repeated field contains a short description of the program name, module name, and offset, in the format described in Table 545. The field is part of the structured repeat group described with FUNCTION_NO.

Table 545. FUNCTION_AT field formats

FUNCTION_AT format	Minor/Major EP	Offset zero
Module	Major	Yes
Module+offset	Major	No
Program in Module	Minor	Yes
Program+offset in Module	Minor	No

Note: The FUNCTION_AT value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_CONTENT

This repeated field contains up to the first 256 bytes of a subsystem function, which usually includes the eye catcher. The default output length of this string is 128 characters, containing the first 128 bytes of the function. In the default output format, the readable text from the contents is shown. The non-printable parts of the contents have been replaced by one or two dots. This field is part of the structured repeat group described by the FUNCTION_NO field.

Note: The FUNCTION_CONTENT value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_KEY

This repeated field contains the storage protection key of a subsystem function, if the residency is in CSA, ECSA, SQA, or ESQA.

A key of 8 is a serious cause for concern because any user can change the subsystem function. A key in the range 9-15 is a minor cause for concern. Only

users running in that key are able to change the subsystem function. Normally, keys 9-15 are used only by controlled applications when running programs from APF libraries. An exception applies to ADDRSPC=REAL. See 1451. This field is part of the structured repeat group described with FUNCTION_NO.

Note: The FUNCTION_KEY value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_LENGTH

If residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA), this repeated field contains the length of the program or module that the function is part of. The field length is approximated as either the length up to the end of the module or the length up to the next entry point. This field is part of the structured repeat group described by the FUNCTION_NO.

Note: The FUNCTION_LENGTH value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_MODULE

If residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA), this repeated field contains the major entry point name of the module in which a subsystem function is located. This field is part of the structured repeat group described by the FUNCTION_NO field.

Note: The FUNCTION_MODULE value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_NO

This repeated field contains the number (index) of a subsystem function. It is a unique key in the FUNCTION structured repeat group, which consists of the following fields:

FUNCTION_NO, FUNCTION_ADDRESS, FUNCTION
FUNCTION_AT, FUNCTION_AMODE, FUNCTION_CONTENT
FUNCTION_KEY, FUNCTION_SUBPOOL, FUNCTION_MODULE
FUNCTION_PROGRAM, FUNCTION_LENGTH, FUNCTION_OFFSET
FUNCTION_SCANINS, FUNCTION_SCANSTR, FUNCTION_WHERE

Note: The FUNCTION_NO value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_OFFSET

If the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA), this repeated field contains the offset from the entry point for the program and the function address, The offset is calculated from the previous entry point. The value is zero if the address is located in a minor or major entry point. This field is part of the structured repeat group described by the FUNCTION_NO field.

Note: The FUNCTION_NO value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_PROGRAM

If the residency is in the LPA (EFLPA, EMLPA, EPLPA, FLPA, MLPA, PLPA), this repeated field contains the entry point name of a subsystem function. If the address is at or just following a minor entry point, this value is the minor entry point name. If the address is at or just following a major entry point, this value

is the major entry point name and is equal to the FUNCTION_MODULE field. The FUNCTION_PROGRAM field is part of the structured repeat group described with FUNCTION_NO.

Note: The FUNCTION_NO value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_SCANINS

This repeated field describes the result of an *instruction scan* performed on the subsystem function code. This field is part of the structured repeat group described by the FUNCTION_NO field. It is only available if the CKFREEZE file used as the data source was produced with the zSecure Collect SCAN=YES parameter. The instruction scan is performed on the full length of the subsystem function, not just on the eye catcher. The scan checks for suspicious instructions in the code.

Note: Interpret the contents of this field as a warning, not as a certainty. The instruction scan can cause false alarms, and can also be fooled to miss certain instructions. Always review the source code of suspicious modules.

Note: The FUNCTION_SCANINS field is only available if the SSVT_ADDRESS field is not zero.

When used for SELECT and EXCLUDE processing, you can use SELECT FUNCTION_SCANINS or SELECT FUNCTION_SCANINS=ANY to select routines in which *any* specified instruction was found. Use SELECT FUNCTION_SCANINS=NONE to select routines in which no specified instructions were found. In addition, you can select routines containing any of the specific instructions listed in the following table, SELECT FUNCTION_SCANINS=(FAKEAPF,FAKESPEC) for example.

Because many suspicious instructions can be found within a single module, the output of this field is in a condensed format. Table 546 lists the FUNCTION_SCANINS values that can be used for SELECT and EXCLUDE processing, the condensed output, and the meaning.

Table 546. FUNCTION_SCANINS field - values and format

SELECT/EXCLUDE	Condensed	Meaning
BYPASS BYPASSSAF	.B.....	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	Set RACF operations authority
FAKEPRIV	......P	Set RACF privileged/trusted authority
FAKESPEC	....S..	Set RACF special authority
KEYZERORB	...0...	For an SVC: modify caller's RB to key-zero
MODESUPRB	..M....	For an SVC: modify caller's RB to supervisor mode

Note: The values printed by the FUNCTION_SCANINS field are subject to change. Do not rely on the exact value of this field in your programs because the content can change.

FUNCTION_SCANSTR

This repeated field describes the result of a *string scan* performed on the subsystem function code. This field is part of the structured repeat group described with FUNCTION_NO. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSTR arguments set. The string scan is performed on the full length of the subsystem function (not just on the eye catcher), and checks for user-specified strings in the code.

The field can have any of the following values: *Yes* if a matching string was encountered in the code. *No* if no such string was found, blank if no string scan was performed.

Note: The FUNCTION_SCANSTR value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_SUBPOOL

This repeated field contains the storage area subpool of a subsystem function if the residency is in CSA, ECSA, SQA, or ESQA. It is part of the structured repeat group described with FUNCTION_NO.

Note: The FUNCTION_SUBPOOL value is only available if the SSVT_ADDRESS field is not zero.

FUNCTION_WHERE

This repeated field contains the residency of a subsystem function. See the SSCT_WHERE field for a reference. This field is part of the structured repeat group described with FUNCTION_NO.

Note: The FUNCTION_WHERE value is only available if the SSVT_ADDRESS field is not zero.

MAX_FUNCTIONS

This field describes the maximum number of function addresses (as opposed to function indices) defined for the subsystem. See the structured repeat group described with the FUNCTION_NO field.

Note: The MAX_FUNCTIONS value is only available if the SSVT_ADDRESS field is not zero.

NAME

The subsystem name. The subsystem name is unique within each system.

ORG, ORDER

The original order in the list of subsystems; this is unique within each system. The *primary* subsystem (usually JES2 or JES3) has ORG value 1.

PSS

This flag field describes the Primary Subsystem Services (PSS) flag, which indicates whether the primary subsystem's services are used when starting this subsystem. If this flag is set (PSS=YES), a START command where the procedure name equals the subsystem name is automatically started under the primary JES. If the flag is not set, the task is automatically started as if SUB=MSTR was specified on the START command.

SSCT_ADDRESS

The address of the subsystem table (SSCT). See also the SSCT_KEY, SSCT_SUBPOOL, and SSCT_WHERE fields.

SSCT_KEY

The storage protection key of the subsystem table, if the table is in CSA, ECSA, SQA, or ESQA. See also the SSCT_ADDRESS, SSCT_SUBPOOL, and SSCT_WHERE fields.

A key of 8 is a serious cause for concern because any user can change the subsystem table. A key of 9-15 is a minor cause for concern. Only users running in that key can change the subsystem table. Normally, keys 9-15 are used only by controlled applications when running programs from APF libraries. An exception applies to ADDRSPC=REAL, see 1451.

SSCT_SUBPOOL

The storage area subpool of the subsystem table if the table is in CSA, ECSA, SQA, or ESQA. See also the SSCT_ADDRESS, SSCT_KEY, and SSCT_WHERE fields.

SSCT_WHERE

The residency of the subsystem table. See also the SSCT_ADDRESS, SSCT_KEY, and SSCT_SUBPOOL fields. Possible SSCT_WHERE values and their meaning are documented in the following table; areas starting with an E reside above the 16 MB line virtual storage. [21]

SSCT_WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

SSVT_ADDRESS

The address of the subsystem's Communication Vector Table (SSVT). See also the SSVT_KEY, SSVT_SUBPOOL, and SSVT_WHERE fields. If zero, the subsystem does not have a communication table; the SSVT_KEY, SSVT_SUBPOOL, and SSVT_WHERE fields, as well as the FUNCTION structured repeat group, are not available.

21. The full Virtual Storage Map is described in the NEWLIST TYPE=VSM.

SSVT_KEY

The storage protection key of the Communication Vector Table (SSVT) for the subsystem if the table is in CSA, ECSA, SQA, or ESQA. See also the SSVT_ADDRESS, SSVT_SUBPOOL, and SSVT_WHERE fields.

A key of 8 is a serious cause for concern because any user can change the SSVT. A key in the range 9-15 is a minor cause for concern. Only users running in that key can change the SSVT. Normally, keys 9-15 are only used by controlled applications when running programs from APF libraries. An exception applies to ADDRSPC=REAL. See 1451.

Note: The SSVT_KEY value is only available if the SSVT_ADDRESS field is not zero.

SSVT_SUBPOOL

Contains the storage area subpool of the Communication Vector Table (SSVT) for the subsystem if the table is in CSA, ECSA, SQA, or ESQA. See also the SSVT_ADDRESS, SSVT_KEY, and SSVT_WHERE fields.

Note: The SSVT_SUBPOOL value is only available if the SSVT_ADDRESS field is not zero.

SSVT_WHERE

The residency of the Communication Vector Table (SSVT) for the subsystem. See also the SSVT_ADDRESS, SSVT_KEY, SSVT_SUBPOOL, and SSVT_KEY fields.

Note: The SSVT_WHERE value is only available if the SSVT_ADDRESS field is not zero.

SUS2_ADDRESS

The SUS2 address. The SUS2 value is treated as a pointer; the derived SUS2 values are invalid if the subsystem uses the SUS2 value for other purposes.

SUS2_CONTENTS

The SUS2 contents. The first 8 characters of the area pointed to by the SUS2 pointer, with non-printable characters replaced by a period.

SUS2_KEY

The storage protection key of the SUS2 pointer if it is in CSA, ECSA, SQA, or ESQA.

A key of 8 is a serious cause for concern because any user can change the SUS2. A key in the 9-15 range is a minor cause for concern. Only users running in that key can change the SUS2. Normally, keys 9-15 are used only by controlled applications when running programs from APF libraries. An exception applies to ADDRSPC=REAL, see 1451.

Note: The SUS2_KEY value is only available if the SUSE_ADDRESS field is not zero.

SUS2_SUBPOOL

The storage area subpool of the SUS2 pointer if it is in CSA, ECSA, SQA, or ESQA.

Note: The SUS2_SUBPOOL value is only available if the SUSE_ADDRESS field is not zero.

SUS2_WHERE

The SUS2 residency. See the SSCT_WHERE field for a reference.

Note: The SUS2_WHERE value is only available if the SUSE_ADDRESS field is not zero.

SUSE_ADDRESS

The SUSE address. The SUSE value is treated as a pointer. The derived SUSE values are invalid if the subsystem uses the SUSE value for other purposes.

SUSE_CONTENTS

The SUSE contents. The first 8 characters of the area pointed to by the SUSE pointer, with non-printable characters replaced by a period.

SUSE_KEY

The storage protection key of the SUSE pointer if it is in CSA, ECSA, SQA, or ESQA.

A key of 8 is a serious cause for concern because any user can change the SUSE pointer. A key between 9-15 is a minor cause for concern. Only users running in a key within that range can change the SUSE pointer. Normally, keys 9-15 are used only by controlled applications when running programs from APF libraries. An exception applies to ADDRSPC=REAL. See 1451.

Note: The SUSE_KEY value is only available if the SUSE_ADDRESS field is not zero.

SUSE_SUBPOOL

The storage area subpool of the SUSE pointer if it is in the CSA, ECSA, SQA, or ESQA.

Note: The SUSE_SUBPOOL value is only available if the SUSE_ADDRESS field is not zero.

SUSE_WHERE

The SUSE residency. See the SSCT_WHERE field for a reference.

Note: The SUSE_WHERE value is only available if the SUSE_ADDRESS field is not zero.

SYSTEM

The name of the system. For MVS systems, the value equals the SMF system ID. The field length is 8 characters for compatibility with other NEWLIST types.

When combined with the ORG or the NAME field, the SYSTEM field uniquely identifies an entry in this NEWLIST type.

TYPE

A string indicating the subsystem type. The value is either JES2 or JES3, or blank.

SVC: Supervisor Calls

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The SVC NEWLIST (NEWLIST TYPE=SVC) describes the MVS SVCs and ESRs, their attributes, and information on previous versions of the SVC read from the SVC

update table. Each entry in this NEWLIST can be uniquely identified by the fields SYSTEM SVCNO ESRNO. If a single system is analyzed, SVCNO ESRNO is a unique key.

Up to five versions of each SVC and derived fields can be found: The current SVC, the old and new versions of the SVC logged in the SVC update table, the SVC as described in the zSecure knowledge base, and routines matching the default name of the SVC (the IPL version). In most cases, some of these versions do not exist, or are equal to another version. Because of this, the SVC NEWLIST groups SVC version-dependent fields into a repeat group, with a single repeat group for each version. An INDEX field indicates which versions are grouped together in a single repeat group entry.

For example, if all versions of an SVC are the same, there is a single repeat group entry. The INDEX field indicates the versions found. If the SVC was updated once using SVCUPDTE, two repeat group entries are listed, one for the current entry and the *new* entry registered in the SVC update table and one matching the *old* entry, the knowledge base, and the IPL version.

The fields included in the SVC NEWLIST fit into one of the following categories:

- Fields describing the overall SVC, which include information like the SVC number or the result of an analysis.
- Fields describing a version of the overall SVC which are repeated once for each different version and described by the INDEX field.
- Fields describing the current SVC. These fields have names starting with CURR_; most are available for every entry (except for some derived fields).
- Fields describing the default or expected SVC, as defined in the zSecure knowledge base and the ***Diagnosis Reference***. These fields have names starting with EXP_, and are available for all default SVCs.
- Fields describing the attributes of the previous SVC, as recorded in the SVC update table. These fields have names starting with OLD_ and are available only if an entry in the SVC update table is available.
- Fields describing the update table, the update date for the table for example. These fields have names starting with UPDATE_ and are available only if an entry in the SVC update table is available.
- Fields describing the caller of the SVCUPDTE service. These fields these have names starting with CALLER_, and are available only if an entry in the SVC update table is available.

Field descriptions

The SVC NEWLIST provides the following fields for reporting.

ADDRESS

This repeated field is part of the structured repeat group described with the INDEX field; it describes the address of the current repeat-group entry. This field is an 8-long (4-byte) hexadecimal number.

AMODE

This repeated field is part of the structured repeat group described with the INDEX field; it describes the addressing mode of the current repeat group entry. This field can have any of the following values: *24*, *31*, *64*.

APPL

The application name of the SVC taken from the internal knowledge base.

AT

This repeated field is part of the structured repeat group described with the INDEX field. The value contains a short description of the program name, module name, and offset, in the format described in Table 547.

Table 547. AT field values

AT format	Minor/Major EP	Offset zero
Module	Major	Yes
Module+offset	Major	No
Program in Module	Minor	Yes
Program+offset in Module	Minor	No

AUDITCONCERN, CONCERN

Indicates the reason for the audit priority. Do not rely on the exact value of this field in your programs as the contents might change. The AUDITCONCERN field can contain one or more concerns separated by commas. Table 548 describes the audit concerns that are currently defined.

Table 548. SVC: Audit concerns and descriptions

Audit Concern	Meaning
APF mismatch	The SVC requires APF authorization according to operating system documentation for this release, but the SVC configuration does not include it. This condition indicates a serious security exposure that can be the result of a hacker creating an unobtrusive back door into the system.
Caller may be unauthorized	Any program can call the SVC. This configuration is true for most SVCs. By itself, it is not a cause for concern, unless the SVC performs sensitive actions. In that case, the SVC must check the authorization of the caller itself. If an installation-defined SVC is configured only for use by authorized programs, it must not be callable by unauthorized programs. Hacking attempts usually focus on this type of SVC.
Code size suspect	The size of the SVC is less than 256 bytes. The small size might indicate inadequate security checks implemented for an SVC that can be called by arbitrary (non-APF) users. A code review is warranted. 90% of a safe SVC is typically spent in user and parameter authorization checking. If the size of the SVC is less than 32 bytes, a *Dangerous code size* concern is issued.
Dangerous code size	The size of the SVC is less than 32 bytes. It is possible that the SVC does not have proper user and parameter authorization checks for the arbitrary (non-APF) caller. A code review is warranted. See also concern *Code size suspect* that is issued if the code size is somewhat larger.
ESR mismatch	The SVC is used as an ESR or an ESR is used as an SVC. This serious concern must be corrected because installation-defined *new* ESRs must not exist, and no system-defined ESR can be redefined as an SVC.
IBM-range SVCno	An SVC has been updated in the range of IBM-defined SVCs, which can be used by all programs or OS services. This concern implies that an IBM-defined SVC has been updated or front-ended. Review the SVC to ensure that the IBM-defined function is still performed and properly protected.

Table 548. SVC: Audit concerns and descriptions (continued)

Audit Concern	Meaning
In application common storage	The actual SVC code has storage key 10, 11, 12, 13, 14 or 15. An application that runs in any of those keys might change it, irrespective of who calls the application. This condition is not as serious as having a storage key of 8 or 9, but it is not as safe as having key 0 storage. Review the application code.
In (E)CSA/(E)SQA	The SVC routine has been added dynamically to the system in non-page protected storage. Typically, this conditions suggests that the routine is part of a third-party product and as such worthy of vulnerability analysis. Also, the routine might not be part of SMP/E or not recognizable as SVC code in SMP/E. As a result, it might have escaped change management procedures normally followed for SVCs. By itself, this condition is not a serious concern.
In (E)FLPA	This indicates code that resides in the Fixed Link Pack Area. The same concerns apply as for MLPA; the difference is that the real storage pages are persistent.
In (E)MLPA	Indicates that the code resides in the Modified Link Pack Area. The software does not reside in the LPA libraries, but has been expressly loaded into MLPA. The most common reasons for this condition are: 1) The code is a test version overruling the PLPA version. 2) The code is not fully reenterable or refreshable or requires modifiable storage because it stores state information. In the first case, you are not running the software configuration (versions) reflected in the SMP/E CSI. In both cases, if the MLPA is not page protected, the software is more vulnerable than in the LPA
In (E)PVT	The SVC was defined in private storage. It can only be used by the owning address space. All other users can run the code occupying the assigned memory area. Invocation of the SVC can result in unpredictable processing, storage overlays, system abends, or hackers taking over the system.
In writable common storage	The SVC is located in a memory area that can be modified by all general users of the system. As a result, the actual code run as part of the SVC processing can be unpredictable, possibly resulting in-storage overlays, system abends, or hackers taking over the system. Immediate action is required.
Installation-defined SVCno	The SVC has no IBM-standard SVC number, and hence is not likely to have been checked by IBM for integrity exposures. On the other hand, if you really need your own SVC, the range of installation-defined SVC numbers is the proper place to define them.
Instruction scan hit (as expected)	The SVC routine contains an instruction that might be used to circumvent normal system security. For example, an instruction that sets a permanently authorized bit from temporarily authorized code, or an instruction that fakes authorization for an unauthorized caller. These things are an exposure if they are not reset before leaving the SVC. Another possible hit is issuing authorized RACF functions that would not be allowed outside the SVC code. All these instruction scan hits warrant a further vulnerability analysis of the SVC code. This concern might be followed by *as expected* when the SVC is known to the program, and known to contain these instructions.

Table 548. SVC: Audit concerns and descriptions (continued)

Audit Concern	Meaning
Known small code size	The size of the SVC is less than 256 bytes. The SVC is known to the program, and known to be this size, so the priority of the SVC is lower than the priorities for other code size concerns like the *Dangerous code size* and *Code size suspect* concerns.
Lock mismatch	The SVC was updated using SVCUPDTE, and the locks required for the current SVC do not match the locks required for the old SVC. If the new SVC front-ends the old SVC, it must acquire or release the locks for the old SVC to function correctly. Review the new SVC to make sure this is the case.
Reserved SVCno	An SVC has been defined in the IBM-reserved range of SVC numbers. This number range must only be used by IBM-defined product-dependent SVCs. Although many third-party vendors use these numbers, their use can lead to conflicts with IBM products.
Same as another SVC	The SVC routine is called by more than one SVC number. This condition is suspicious unless it is the error SVC. It is especially suspicious if one copy requires APF authorization and the other does not.
String scan hit	The SVC routine contains a string specified or implied in the zSecure Collect run. The default string for such a run is an instruction sequence that is unsafe when the routine has the `AC(1)` attribute instead of the correct `AC(0)` attribute.
Suspected frontending	The SVC routine is not installation defined, but nonetheless stored in (E)CSA or (E)SQA. IBM supplied SVCs are never stored in (E)CSA, so this warrants a careful examination.
Suspect SVC inst	The SVC starts with another SVC instruction. Being part of another SVC, the called SVC can bypass normal authorization verifications. Resulting processing can cause a circumvention of normal system integrity controls exploitable by hackers.
SVC scan hit (as expected)	This SVC calls another SVC that is dangerous. Analyze the SVC code to verify that it does not simply pass a user-specified parameter list but only authorizes very specific functions that cannot be misused. The exact list of SVCs scanned for is set by the zSecure Collect parameter `SCANSVC`. The default for that parameter is the SVC codes for the resident security system (RACF or ACF2). This concern can be followed by *as expected* when the SVC is known to the program and known to call these SVCs. In that case, the audit priority is lower.
Type mismatch	The SVC should be defined as a different type than it was actually found in the system (Based on the operating system documentation for the specific release, the SVC type is not defined correctly. This condition might result in incorrect processing, but usually this condition is caused by a documentation error or backlog.
Unsafe branch	The SVC uses a register whose contents are caller-specified as index or base for a branch instruction. The branch location is therefore not predictable by the SVC code. Running the SVC can result in unpredictable processing, storage overlays, system abends, or hackers taking over the system.

Table 548. SVC: Audit concerns and descriptions (continued)

Audit Concern	Meaning
Unsafe STM	The SVC stores several registers at the location pointed to by Register 13. This condition is common coding practice for normal user programs. For SVCs, the contents of register 13 is caller-specified. The SVC might cause storage overlays resulting in unpredictable behavior, system abends, or hackers taking over the system.
Updated during NIP	The SVC table has been changed, but the change occurred during Nucleus Initialization Processing, probably as part of regular link pack area creation. This change does not contribute to the audit priority and indicates that the change is nothing to worry about.
Updated twice in RACF startup	The SVC table has been changed twice, but these changes are normal for RACF startup processing of RACF SVCs. This change does not contribute to the audit priority and indicates that the SVCUPDTE change is nothing to worry about.
Updated using SVCUPDTE	The SVC was updated using the SVCUPDTE service. This SVC routine is not the original code as installed under the module name used for this SVC number by default. The routine has been changed dynamically through the documented dynamic SVC update procedure SVCUPDTE. If this concern is issued in connection with an IBM SVC, the installed code is usually a frontend to the regular SVC.
Updated without SVCUPDTE	SVC routine is not the original code as installed under the module name used for this SVC number by default, but has been changed dynamically. The change has not been done through the documented dynamic SVC update procedure, pointing to possibly dangerous coding practices by the software vendor. If this concerns an IBM SVC, the installed code is usually a 'front-end' to the regular SVC. The new SVC must be reviewed.

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 549. SVC NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

CALLER_ADDRESS

The address of the last caller of the SVCUPDTE service, as a 4 byte hexadecimal number. This field is only available if an entry in the update table is available for the current SVC.

From the caller address, the CALLER_AT and CALLER_WHERE fields are derived.

CALLER_AT

The entry point location at the caller address. This field is available only if an entry in the update table is available for the current SVC. See also the CALLER_ADDRESS and CALLER_WHERE fields; see the AT field for a reference.

CALLER_WHERE

The residency of the memory area at the caller address. This field is only available if an entry in the update table is available for the current SVC. See also the CALLER_ADDRESS and CALLER_AT fields. See the WHERE field for a reference.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. This value can be taken from the ALLOC COMPLEX parameter or default to a system name.

CONTENTS

This repeated field is part of the structured repeat group described with the INDEX field; it describes the contents of the current repeat group entry. This field is a string containing up to the first 256 bytes of the SVC, which usually include the eye catcher. In the default output format, the readable text from the contents is shown. The non-printable parts of the contents have been replaced by one or two periods (. or ..) .

CURR_ADDRESS

The entry point of the current SVC, as a 4 byte (8 positions) hexadecimal number. See also the ADDRESS field.

CURR_AMODE

The addressing mode of the current SVC. This field can have the following values: *24* or *31*.

CURR_APF

Flag indicating whether the current SVC requires the caller to be APF-authorized.

CURR_AT

This field contains a short description of the program name for the current SVC, module name, and offset in the format described by the AT field.

CURR_ATTR

The SVC attributes (other than APF, ESR, and LOCKS). This is a three-position character field with the following values:

ATTR value	Meaning
A	SVC can be run in Access Register mode
N	SVC cannot be preempted
S	SVC can be assisted by hardware

CURR_CONTENTS

A string containing up to the first 256 bytes of the current SVC code, which usually include the eye catcher. The default output length of this string is 128 characters (containing the first 128 bytes of the SVC code). In the default output format, the readable text from the contents is shown. The non-printable parts of the contents have been replaced by one or two periods (. or ..). See also the CONTENTS field.

CURR_ESR

Flag indicating whether the current SVC is an ESR entry.

Note: An SVC table entry that points to an ESR table is not included as an entry.

CURR_KEY

The storage protection key of the memory area at the entry point for the current SVC. That is, at the CURR_ADDRESS. See also the KEY field.

CURR_LENGTH

The length of the current SVC program; see also the LENGTH field.

CURR_LOCK

This field describes the system locks required by the SVC. It contains a character for each lock type required, and a blank for each lock type not required. This field has the format CDLOS; the meaning of these characters is described in Table 550.

Table 550. CURR_LOCK values

Character	SVC lock types
C	CMS
D	DISP
L	LOCAL
O	OPT
S	SALLOC

CURR_MODULE

This field contains the major entry point name for the current SVC.

CURR_OFFSET

This field contains the offset between the entry point for the current SVC and the next prior entry point. See the OFFSET field.

CURR_PROGRAM

This field contains the major entry point/minor entry point name for the current SVC. See the PROGRAM field.

CURR_RESULT

This field contains the result of the SVC disassembly. Currently, only the 'do-nothing' program IEFBR14, the error SVC, and the error ESR are recognized. See the RESULT field.

CURR_SAME_AS

This field contains the first SVC or ESR that has the same entry point as the current SVC. It has the format 'SVC 100' or 'ESR 109/24'. See the SAME_AS field.

CURR_SCAN_INSTR

This field describes the result of an *instruction scan* performed on the code for the current SVC. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter. The instruction scan is performed on the full length of the SVC (not just on the eye catcher), and checks for suspicious instructions in the code.

Note: Interpret the contents of this field as a warning, not a certainty. The SVC scan can cause false alarms and can also be fooled to miss certain SVC calls. Always review the source code of suspicious modules.

When used for SELECT and EXCLUDE processing, you can use SELECT CURR_SCAN_INSTR or SELECT CURR_SCAN_INSTR=ANY to select routines in which *any* instruction was found; use SELECT CURR_SCAN_INSTR=NONE to select routines in which no instructions were found. In addition, you can select routines containing any of the specific instructions listed in Table 551, SELECT CURR_SCAN_INSTR=(FAKEAPF,FAKESPEC) for example.

Because many suspicious instructions can be found within a single module, the default output of this field is in a condensed format. Full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 9, CURR_SCAN_INSTR(EXPLODE,9 for example. Table 551 lists the CURR_SCAN_INSTR values that can be used for SELECT/EXCLUDE processing; the condensed output; the exploded output; and the meaning.

Table 551. CURR_SCAN_INSTR values

Select/Exclude	Condensed	Exploded	Meaning
BYPASS BYPASSSAF	.B.....	BypassSAF	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	FakeAPF	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	FakeOper	Set RACF operations authority
FAKEPRIV	......P	FakePriv	Set RACF privileged/trusted authority
FAKESPEC	....S..	FakeSpec	Set RACF special authority
KEYZERORB	...0...	KeyzeroRB	For an SVC: change the RB for the caller to key-zero
MODESUPRB	..M....	ModeSupRB	For an SVC: change the RB for the caller to supervisor mode

Note: The values printed by the CURR_SCAN_INSTR field are subject to changes in future releases. Do not write applications that are dependent on the output of this field.

CURR_SCAN_STRING

This field describes the result of a *string scan* performed on the SVC code. It is only available if the CKFREEZE file used was produced with the SCAN=YES

parameter and SCANSTR arguments set. The string scan is performed on the full length of the SVC (not just on the eye catcher), and checks for user-specified strings in the code.

The value of this field is set to *Yes* if a matching string was encountered in the code; *No* if no such string was found; the field is left blank if no string scan was performed.

CURR_SCAN_SVC

This repeated field describes the result of an SVC scan performed on the SVC code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSVC list of SVC numbers set. The SVC scan is performed on the full length of the SVC not just on the eye catcher and also checks for user-specified SVC calls in the code.

Note: Interpret the contents of this field as a warning, not a certainty. The SVC scan can cause false alarms and can also be fooled to miss certain SVC calls. Always review the source code of suspicious modules.

The value of this field has the format `num: description` if the SVC scanned for was one of the first seven specified in zSecure Collect. If any of the other SVCs scanned for was encountered, this field has the value *Other*.

CURR_SUBPOOL

This field contains the storage area subpool of the current SVC, if the residency is in CSA, ECSA, SQA, or ESQA. See the SUBPOOL field.

CURR_TYPE

The type of the current SVC. This field is 3 characters long and can have any of the following values: *1*, *2*, *3/4*, or *6*. The SVC type determines the module naming convention.

CURR_WHERE

String field that indicates the virtual storage area where the current `SVC` resides. See the `WHERE` field.

ESRNO

This field is undefined for a normal SVC. If the current `SVC` is an extended SVC as indicated by the `ESR=YES`, this field contains the `ESRNO` table index. This value is the number passed in R15 when the SVC is called.

EXP_APF

Flag field that indicates if the expected SVC (from the database) with the current `SVCNO` and `ESRNO` requires the caller to be APF-authorized.

EXP_ESR

Flag field that indicates if the expected `SVC` (from the database) with the current `SVCNO` is an ESR entry.

EXP_PROGRAM

The program name of the expected SVC (from the database) with the current `SVCNO` and `ESRNO`.

EXP_TYPE

The type of the expected SVC (from the database) with the current `SVCNO`. This field is 3 characters long and can have any of the following values: *1*, *2*, *3/4*, or *6*.

FUNCTION

A string of up to 80 characters describing the function of the SVC. If this function is not directly defined, a guess is made based on the value of the PROGRAM field. This guess is printed enclosed in brackets.

INDEX

This repeated field is the anchor for a large group of repeated fields that describe one or more versions of the SVC. It indicates which versions of the SVC are described in these repeated fields. The INDEX field value can be a maximum of 4 characters, each indicating one version. The letters are arranged in reverse chronological order. That is, the most recent version first.

Index	Meaning
C...	The current SVC, for example, the version that is used if an SVC call is issued.
.N..	The new SVC as registered in the SVC update table. This value can only occur if the SVC was updated at least once using SVCUPDTE. The *new* version is always equal to the current version, unless the SVC was updated again without using SVCUPDTE.
..O.	The previous *old* SVC as registered in the SVC update table. This index value can only be returned if the SVC was updated at least once using SVCUPDTE. The *old* version is often equal to the IPL version if the SVC was updated once.
...I	The IPL version of the SVC. That is, the in-storage module matching the name that the SVC had before any updates were performed.

INDEXCOUNT

This field describes the number of entries in the structured repeat group described with the INDEX field.

KEY

This repeated field is part of the structured repeat group described with the INDEX field. It describes the storage protection key of the memory area at the entry point, or corresponding address for the SVC if the residency is in CSA, ECSA, SQA, or ESQA.

A key of 8 is a serious cause for concern because any user might be able to change the SVC code. A key of 9 to 15 is a minor cause for concern. Only users running in that key are able to change the SVC code. Keys 9 - 15 can normally be used only by controlled applications when running programs from APF libraries. An exception goes for ADDRSPC=REAL. See 1451.

LENGTH

This repeated field contains the length of the program/module the SVC is part of, if the residency is in the LPA or nucleus. (The length is approximated as the length up to the end of the module, or the length up to the next entry point.) It is part of the structured repeat group described with the INDEX field.

MODULE

If the residency is in the LPA or nucleus, this repeated field contains the major entry point name of the module in which the SVC is located. It is part of the structured repeat group described with the INDEX field.

OFFSET

If the residency is in the LPA or nucleus, this repeated field contains the offset from the entry point for the program and the SVC entry point. The offset is

calculated from the previous entry point. It is zero if the address is located in a minor or major entry point. The OFFSET field is part of the structured repeat group described by the INDEX field.

OLD_APF

Flag field that indicates if the previous SVC (the old entry in the SVC update table) required the caller to be APF-authorized.

OLD_ATTR

The previous SVC (the old entry in the SVC update table) attributes (other than APF, ESR, and LOCKS). See the CURR_ATTR field.

OLD_ESR

Flag field that indicates if the previous SVC was an ESR entry. The previous entry is the old entry in the SVC update table.

OLD_LOCK

Describes the system locks required by the previous SVC. The previous entry is the old entry in the SVC update table. See the CURR_LOCK field for a reference.

OLD_TYPE

The type of the previous SVC. The previous entry is the old entry in the SVC update table. This field is 3 characters long and can have any of the following values: *1*, *2*, *3/4*, or *6*.

PROGRAM

This repeated field contains the entry point name of an SVC if the residency is in the LPA or nucleus. If the address is at or just following a minor entry point, this value is the minor entry point name. If the address is at or just following a major entry point, this value is the major entry point name and is equal to the MODULE field.

The PROGRAM field is part of the structured repeat group described with the INDEX field.

RESULT

This repeated field is part of the structured repeat group described using the INDEX field. It contains the result of the SVC disassembly. Currently, the following values are recognized: The *do-nothing* program IEFBR14– which is the default program in use as ESR 109/36 that just sets RC=4, the error SVC, and the error ESR.

SAME_AS

This repeated field is part of the structured repeat group described with the INDEX field. It contains the first SVC or ESR that has the same entry point as the current entry. It has the format 'SVC 100' or 'ESR 109/24'.

SCAN_INSTR

This repeated field is part of the structured repeat group described with the INDEX field. It describes the result of an *instruction scan* performed on the SVC code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter. The instruction scan is performed on the full length of the SVC (not just on the eye catcher), and checks for suspicious instructions in the code.

Note: Interpret the contents of this field as a warning, not a certainty. The SVC scan can cause false alarms and can also be fooled to miss certain SVC calls. Always review the source code of suspicious modules.

When used for SELECT or EXCLUDEprocessing, you can use SELECT SCAN_INSTR or SELECT SCAN_INSTR=ANY to select routines in which *any* specified instruction was found. Use SELECT SCAN_INSTR=NONE to select routines in which no specified instructions are found. In addition, you can select routines containing any of the specific instructions listed in Table 552, SELECT SCAN_INSTR=(FAKEAPF,FAKESPEC) for example.

Because many suspicious instructions can be found within a single module, the output of this field is in a condensed format. Table 552 lists the SCAN_INSTR values that can be used for SELECT and EXCLUDE processing, the condensed output, and the meaning.

Table 552. SCAN_INSTR values for SELECT and EXCLUDE processing

SELECT/EXCLUDE	Condensed	Meaning
BYPASS BYPASSSAF	.B.....	Request DFP (DFSMS) to bypass SAF calls
FAKEAPF	A.....	Fake APF/AC(1)-authorization
FAKEOPER	.....O.	Set RACF operations authority
FAKEPRIV	......P	Set RACF privileged/trusted authority
FAKESPEC	....S..	Set RACF special authority
KEYZERORB	...0...	For an SVC: change the RB for the caller to key-zero
MODESUPRB	..M....	For an SVC: change the RB for the caller to supervisor mode

Note: The values printed by the SCAN_INSTR field are subject to changes in future releases. Do not write applications that are dependent on the output of this field.

SCAN_STRING

This repeated field is part of the structured repeat group described with the INDEX field. It describes the result of a *string scan* performed on the SVC code. It is only available if the CKFREEZE file used was produced with the SCAN=YES parameter and SCANSTR arguments set. The string scan is performed on the full length of the SVC (not just on the eye catcher), and checks for user-specified strings in the code.

The value of this field is set to *Yes* if a matching string was encountered in the code. The value is *No* if no such string was found. The field is left blank if no string scan was performed.

SUBPOOL

This repeated field contains the storage area subpool of an SVC, if the residency is in CSA, ECSA, SQA, or ESQA. It is part of the structured repeat group described with the INDEX field.

SVCNO

The SVC number. For extended SVCs, see the ESRNO field.

SYSTEM

The name of the system. For MVS systems, this value is equal to the SMF system ID. The field length is 8 characters for compatibility with other NEWLIST types.

UPDATE_COUNT

The number of times the SVC has been updated, as registered in the SVC update table.

UPDATE_CURRENT

Flag field that indicates if the SVC update table describes the latest change to the SVC. That is, the time that the SVC was changed using SVCUPDTE, but not changed since. This value is set if both the ADDRESS and the attributes match, if the NEW entry is suppressed in all repeated fields for example.

UPDATE_DATE

The date of the last SVC update registered in the SVC update table. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

UPDATE_SUFFIX

This field contains a two-character suffix indicating a parmlib member. It is taken from the SVC update table, and is only set if the SVC was updated through a parmlib IEASVCxx member. In this case, the update suffix contains the last two characters of IEASVCxx **01** for IEASVC01 for example.

WHERE

This repeated field is part of the structured repeat group described with the `INDEX` field. It describes the residency of the current repeat-group entry. Table 553 lists the possible `WHERE` values and their meaning. Areas starting with an `E` reside above the 16 MB line in virtual storage.

Note: The full Virtual Storage Map is described in the `VSM NEWLIST`.

Table 553. WHERE values and descriptions

WHERE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area

Table 553. WHERE values and descriptions (continued)

WHERE value	Meaning
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area

SYSTEM: System-wide Options

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The SYSTEM NEWLIST type provides information about system-wide option settings. System information is reported with one entry per system. Unless otherwise stated, all fields are supported in SELECT and EXCLUDE statements and the following output commands: LIST, SORTLIST, DISPLAY and SUMMARY.

The SYSTEM NEWLIST does not support the AUDITCONCERN keyword because the amount of information to include in display panels and reports is too large. For information on system audit information, see "AUDIT: System setting audit concerns" on page 961.

Field descriptions

The SYSTEM NEWLIST supports the following fields for reporting.

ADSP, SETRADSP, SYSTEMADSP

This RACF flag indicates whether Automatic Data Set Protection (ADSP) is in effect (due to a SETROPTS ADSP command). If set (ADSP=YES), RACF creates a discrete profile for each new data set created by users that have the ADSP attribute on their user profile or on their current connect group. If not set, individual user or connect group ADSP attributes are not honored. This field supports overtype.

AIM_DB_STAGE

Specifies the implementation stage for the Application Identity Mapping feature of RACF. For systems not running RACF this field is missing.

AIM_SMF_RECNO

Contains the SMF record type written by the Proginet SecurPass Audit Information Manager.

APPLAUDIT

Flag field that indicates ifAPPC transactions are audited through the APPL class.

If this keyword is set to *YES*, the start and end of an APPC transaction is audited. This setting only applies when an APPL class is present that has success auditing activated.

If the APPLAUDIT keyword is not specified, APPC start and end events are not audited.

This option setting can also be specified by the SETROPTS APPLAUDIT command.This field supports overtype.

AUDIT_GROUP

Flag field that indicates if RACF is logging all RACF commands and DEFINE requests affecting profiles in the GROUP class. These commands are ADDGROUP, ALTGROUP, CONNECT, DELGROUP, and REMOVE. It reflects the SETROPTS AUDIT(GROUP) setting. This field supports overtype.

AUDIT_USER

Flag field that indicates ifRACF is logging all RACF commands and DEFINE requests affecting profiles in the USER class. These commands are ADDUSER, ALTUSER, CONNECT, DELUSER, PASSWORD, and REMOVE. It reflects the SETROPTS AUDIT(USER) setting. This field supports overtype.

BATCHALLRACF

This RACF flag indicates whether JES is only to accept jobs containing either a valid RACF userid and password or propagated RACF information. If BATCHALLRACF=YES is specified, any job not containing this user identification fails. If this setting is not active, jobs without a RACF user ID run with default authority access based on the permissions defined in the UACC and the Global Access Table.

The option indicated by this flag can be set by a SETROPTS JES(BATCHALLRACF) command. This field supports overtype.

CA1_BATCH

Flag field that indicates if the CA-1 option BATCH is active. It controls access to the TMC Volume and DSNB record(s) in conjunction with the YSVC option, as shown in the CA1_YSVC field. When BATCH is active a second access check is done if the check done for the YSVC option results in conditional access. For rename actions, a third access check is done. These extra checks are done in the DATASET class, with the data set name retrieved from the TMC. For rename operations, a check is also done on the new data set name.

CA1_CREATE

Character string that specifies the access level needed to create a tape. For CA-ACF2 and CA-TopSecret, specify *CREATE* for this setting. For RACF, specify *ALTER*.

CA1_DSE

Flag field that indicates if the CA-1 option DSEALL is active (Data Security Erase). If set, the tape must have been erased by TMSTPPRO with an ERASE parameter before it can be reused.

CA1_DSNB_EFFECTIVE

Flag field that indicates if the CA-1 options `DSNB` and `OCEOV` are both active. If active, then each access to a secondary tape data set results not only in an access check for the data set in question, but also in an access check for the first data set on the tape. This access check is issued as an SAF call for class `DATASET` with the full 44-character data set name of the first file on the first volume of the multi-volume complex. This data set name comes from the CA-1 Tape Management Catalog. The `UNDEF` option, as shown in the `CA1_UNDEF_FAIL` field, regulates what happens when SAF returns RC 4.

CA1_FORNDSN

Contains the value of the CA-1 option FORNDSN. It can be ALL, INPUT, OUTPUT or NONE, indicating for which type of access to nonresident tapes access checks are done in the DATASET class.

CA1_FUNC

Flag field that indicates if the CA-1 option FUNC is active. This option setting causes real-time resource checks for occurrences of the EXPDT=98000 parameter and for use of the following label types: NL, NSL, and BLP.

CA1_OCEOV

Flag field that indicates if the CA-1 option OCEOV is active. If active, then each access to a tape data set results in a SAF call for class DATASET with the full 44-character data set name from the CA-1 Tape Management Catalog. The UNDEF option, as shown in the CA1_UNDEF_FAIL field, regulates what happens when SAF returns RC 4.

CA1_PSWD

Flag field that indicates if the CA-1 option PSWD is active. If active, the user of an online access password must pass a resource check against that password in class CATAPE. The UNDEF option, as shown in the CA1_UNDEF_FAIL field, regulates what happens when SAF returns RC 4.

CA1_UNDEF_FAIL

Flag field that indicates if the CA-1 option UNDEF is set to FAIL. This option regulates whether an "undecided" return code from SAF results in a refusal.

CA1_YSVC

Flag field that indicates if the CA-1 option YSVC is active. If active, then callers of the CA-1 SVC must pass a resource check against YSVCUNCD (for unconditional access) or YSVCCOND (for conditional access) in class CATAPE. When YSVCCOND access is granted, extra checks are performed when the BATCH option is active. When the BATCH option is inactive, conditional access is denied. The UNDEF option, as shown in the CA1_UNDEF_FAIL field, regulates what happens when SAF returns RC 4.

CATDSNS

This string indicates whether RACF prevents users from accessing uncataloged, new or system temporary data sets. It reflects an option set by a SETROPTS CATDSNS command. The following table documents the CATDSNS values, the corresponding SETROPTS commands, and their meanings.

CATDSNS value	SETROPTS command	Meaning
No	SETROPTS NOCATDSNS	Uncataloged data sets are not protected from access
Warning	SETROPTS CATDSNS(WARNING)	Access to uncataloged data sets is permitted but generates a warning
Yes/Fail	SETROPTS CATDSNS(FAILURES)	Access to uncataloged data sets is only permitted for started tasks and SPECIAL users. Access for other users is not permitted.

This field supports overtype.

CKRSITE_CLASS

This text field indicates the general resource class that was specified in the CKRSITE module that was active at the moment the CKFREEZE file was created.

CMDVIOL

This RACF flag indicates whether RACF is to log violations detected by RACF commands (due to a SETROPTS CMDVIOL command). If set (CMDVIOL=YES), command violations are logged. This field supports overtype.

COLLECTDATE

A string of 17 characters containing the time stamp of the zSecure Collect file for the current system, in the format `DD MMM YYYY HH:MM`, indicating day, month, year, and time.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPATMODE

This RACF flag indicates whether RACF is to allow users and jobs that do not have security labels on a system enforcing security labels (due to a SETROPTS COMPATMODE command). If set (COMPATMODE=YES), RACF allows users and jobs without security labels. This field supports overtype.

COMPLEX

The security complex that contains the system. This can come from the ALLOC COMPLEX parameter or default to a system name.

CON_AMRF

This flag field indicates whether the Action Message Retention Facility (AMRF) is active. This is specified by the INIT,AMRF parameter in parmlib member CONSOLxx. If set, action messages are kept in a buffer, so that they can be review using the DISPLAY R,M command.

CON_CMDDELIM

This field contains the installation's command delimiter. This is specified by the INIT,CMDDELIM parameter in parmlib member CONSOLxx.

CON_CONSOL

Contains the parmlib CONSOL*xx* member suffix for reading console, syslog, and hardcopy definitions. For example, `CON_CONSOL=00` indicates parmlib member `CONSOL00`.) The parmlib member suffix is specified by the `CON` parameter of parmlib member `IEASYS`*xx*.

Logically, the `CON` parameter contains the active setting, while the IPL specification is in `IPLPARM_CON`. However, because the `CON` parameter is not dynamic the values are the same.

CON_DFLT_ROUT

This field indicates the default routing codes for messages that do not have routing information. This is specified by the DEFAULT,ROUTCODE parameter in parmlib member CONSOLxx.

CON_HCPY_CMDLVL

This field contains the type of commands to be recorded on hardcopy. This is specified by the HARDCOPY,CMDLEVEL parameter in parmlib member CONSOLxx. Table 554 on page 1433 lists the possible values for this field.

Table 554. Types of commands that can be recorded in printed output

Value	Meaning
CMDS	Operator commands, system commands, responses, static status displays, and time-interval updates status displays are logged.
INCMDS	Operator commands, system commands, and responses are logged.
NOCMDS	No commands, responses, or status displays are logged.
STCMDS	Operator commands, system commands, responses, and static status displays are logged.

CON_HCPY_DEVNUM

This field indicates whether the hardcopy log is sent to syslog (*SYSLOG*) or to a hardcopy log device (*nnn*). The device number value is taken from the HARDCOPY,DEVNUM parameter in parmlib member CONSOL*xx*. It is not the actual device number.

CON_HCPY_ROUT

Indicates the message routing codes the hardcopy log is to receive. This value is specified by the HARDCOPY,ROUTCODE parameter in parmlib member CONSOLxx.

CON_LOGON_AUTO

This flag field indicates whether a logon is automatic for the system consoles. This is specified by the DEFAULT,LOGON parameter of parmlib member CONSOLxx. If set, each console that is activated is logged on using the console's name as userid.

CON_LOGON_REQ

This flag field indicates whether a logon is required for the system consoles. This is specified by the DEFAULT,LOGON parameter of parmlib member CONSOLxx. If not set, no logon is required for system consoles; if any system console resides in a physically insecure area, this is a security exposure. B1 security requires a logon.

CON_MLIM

This field indicates the maximum number of buffers that can be used for WTO messages. This is specified by the INIT,MLIM parameter in parmlib member CONSOLxx.

CON_MON_DSNAME

This flag field indicates whether the system adds information on the first non-temporary data set allocated on a DASD volume to mount messages displayed on consoles. This is specified by the INIT,MONITOR parameter in parmlib member CONSOLxx.

CON_MON_SPACE

This flag field indicates whether the system adds information on the space available on a DASD volume to mount messages displayed on consoles. This is specified by the INIT,MONITOR parameter in parmlib member CONSOLxx.

CON_MONITOR

This field shows the events that must be monitored for the purpose of automation, like JOBNAMES, SESSION, and STATUS. It is set by the MVS command SETCON MONITOR. The MONITOR option allows you to receive monitored messages for automation purposes without requiring that the

messages be queued to a console or be written to SYSLOG or OPERLOG. This field can be displayed with output formats MONITOR and $MONITOR; the default format is MONITOR and the default output width is 5.

CON_MPFLST

This field contains the parmlib MPFLSTxx member suffix used to read Message Processing Facility (MPF) definitions. (Value <pv>00</pv> indicates parmlib member MPFLST00.) This is specified using the INIT,MPF parameter of parmlib member CONSOLxx.

You can specify multiple MPFLSTxx members. You can also display the MPFLSTxx members used using the MPF report.

CON_MSG_LOSS

This flag field indicates whether messages have been lost somewhere in the sysplex. If set, the message procedures can be in error, and the events described by the messages cannot be audited using the system log.

CON_PFKTAB

This field contains the parmlib PFKTABxx member suffix used to read console function key definitions. (Value <pv>00</pv> indicates parmlib member PFKTAB00.) This is specified using the INIT,PFK parameter of parmlib member CONSOLxx.

CON_RLIM

This field indicates the maximum number of buffers that can be used for WTOR messages. This is specified by the INIT,RLIM parameter in parmlib member CONSOLxx.

CON_UEXIT

This flag field indicates whether the WTO(R) installation exit IEAVMXIT is to be active. This is specified by the INIT,UEXIT parameter in parmlib member CONSOLxx.

CPU_MODEL_BYTE

This parameter identifies the two–character CPU model byte, a model within the CPU_TYPE. This is not the model as it can be found in brochures, but the byte as it is returned by the hardware.

If the data is generated by an APF-Authorized zSecure Collect program run on MVS, the program usually obtains the model byte value from VM.

To get the correct value for the model byte, you need a CKFREEZE file created by an APF-authorized run of the zSecure Collect program which retrieves the actual model data from the system.

If you do not use such a CKFREEZE file or obtain the value from a non-APF authorized CARLa query (run from the zSecure product panel, for example) and your z/OS system runs on a virtual machine, the CPU_MODEL_BYTE value returned is `FF`. This value represents the z/VM model byte for a virtual machine, not the actual model for the z/OS system.

CPU_MODEL_NAME

Contains the CPU model identification as reported by the CSRSI service. The value is typically shown in the following format: *`manufacturer type`* `model` *`model`*. The value is missing on systems that do not have the CSRSI service.

CPU_SERIAL

5 character CPU serial. This number is usually a unique number within machines with the same CPU_TYPE. For certain CPU types, the model can be set by the customer (for example, a P/390). For a machine with LPARs or their OEM equivalent, the first digit usually identifies the LPAR number. The processor number (the first digit of the hardware processor serial number - LPAR is the second digit) is not reported.

CPU_TYPE

4 character CPU type as returned by the processor hardware.

DATE_OFFSET

Returns the offset between the UTC date and the local date as set with the SET DATE system command. The value is specified in number of days.

DASDVOL

This RACF flag indicates whether the DASDVOL class is active. If set (DASDVOL=YES), users that do not have ALTER access to a data set are still able to alter, rename, delete, dump and restore the data set if they have access to a profile in the DASDVOL class for the volume containing the data set.

DEVSUP_TAPEAUTHDSN

This flag indicates how DFSMS issues SAF calls to verify authorization to a tape data set. If this flag is on, SAF calls are issued in the DATASET class that are identical to those issued if the data set resided on DASD (except for the volume serial). If this flag is off, SAF calls are issued with the DSTYPE=T option set, which means that special tape protection options come into play.

DEVSUP_TAPEAUTHF1

Flag field that indicates ifDFSMS issues an additional SAF call to verify authorization to the first data set on a tape when accessing another data set residing on the tape.

DFPLEVEL

A string that indicates the software level of Data Facility Product (DFP) . For Data Facility Storage Management Subsystems (DFSMS), the DFP level is stabilized to level 3.3.1.

DEVSUP_TAPEAUTHRC4

This string, which can be ALLOW or FAIL, indicates whether DFSMS denies access to data sets that are not protected by a security profile when TAPEAUTHDSN or TAPEAUTHF1 are in effect.

DEVSUP_TAPEAUTHRC8

String that indicates whether DFSMS is running in warning mode when the `TAPEAUTHDSN` or `TAPEAUTHF1` setting is specified. This setting can have the following values:

- WARN means that access is permitted to data sets that typically cannot be accessed. Your security product reports the access as a violation. However, the `OPEN` and `EOV` actions are permitted.
- `FAIL` means that the access attempts fail.

DLOGOPT

Auditing options for data sets (RACFclass=DATASET), due to a SETROPTS LOGOPTIONS command. The DLOGOPT values and the SETROPTS LOGOPTIONS auditing level are documented in the table below.

DLOGOPT value	SETROPTS LOGOPTIONS auditing level
Always	ALWAYS
Failure	FAILURES
Never	NEVER
Profile	(determined by profile)
Success	SUCCESSES

Use the LOGOPT field of NEWLIST TYPE=CLASS to display auditing options for all classes.

DMS parameters

Note that for this and all subsequent DMS parameters the value can only be trusted if zSecure Collect was able to find the parameter data set and member. If not, some values are set to the DMS-documented default value and others are simply empty. If some parameters are empty, do not trust the other values.

DMSRACFALWZ

String value that shows value of the DMS RACFALWZ (RACF always-call) parameter. This setting indicates whether RACF support is called for non-indicated data sets. On systems that have DFP, specify `DMSRACFALWZ=Y`

If `DMSRACFALWZ=N`, then data sets that are not RACF-indicated are processed by DMS without further security checking.

If this string is set or if the data set is indicated, the actions of DMS are further determined by the `RACFSUPP` parameter. See the `DMSRACFSUPP` keyword description.

DMSRACFBKUP

String value that shows the `DMS RACFBKUP` (RACF discrete profile backup) parameter. This parameter determines if DMS backs up discrete profiles to a profile with a generated name. The generated name has the format *`userid`*`.jobname.Dyyddd.THMhhmm.TSSssth`, where *`userid`* is the qualifier defined by DMS parameter `RACFUSID` represented by the `DMSRACFUSID` keyword. The possible `DMSRACFBKUP` values and their meaning are defined in the Table 555.

Table 555. SYSTEM NEWLIST TYPE - possible values for the DMSRACFBKUP keyword

DMSRACFBKUP value	Meaning
`F`	DMS never saves profiles.
`N`	DMS never saves profiles at backup and archive.
`Y`	DMS saves profiles for archive but not for backup.

The values `Y` and `F` provide incomplete discrete profile support. Data sets that have a discrete profile during archive/backup cannot be restored.

DMSRACFDVOL

The DMS parameter RACFDVOL shows the volume serial number used in backed up discrete profiles. (See also the DMSRACFBKUP keyword description.

DMSRACFNEWN

The DMS parameter RACFNEWN (RACF new-name) indicates if data sets can be renamed when they are restored. Specifying DMSRACFNEWN=Y results in a security exposure because DMS only checks access on the target (new) data set name, not on the name being restored.

DMSRACFPRED

The DMS parameter RACFPRED indicates whether DMS pre-defined discrete profiles are used during restore.

DMSRACFPROC

Indicates if the DMS/OS RACF interface for RACF processing is activated.

- DMSRACFPROC=Y indicates that DMS bypasses RACF-indicated data sets without a profile. If the setting DMSRACFALWZ=Y is also specified, DMS bypasses all data sets without a profile.
- DMSRACFPROC=N indicates that DMS processes RACF-indicated data sets even if no profile exists. If the setting DMSRACFALWZ=Y is also specified, DMS process all data sets even if no profile exists.

DMSRACFSUPP

This DMS parameter indicates whether DMS processes data sets ('RACF Support'). If not set (DMSRACFSUPP=N), RACF-indicated data sets (or all data sets if RACFALWZ=Y) are *not* processed (for example, they are not restored or backed up). If set (DMSRACFSUPP=Y), processing depends on the DMS parameter RACFPROC (see field DMSRACFPROC).

DMSRACFUSID

This DMS parameter RACFUSID shows the first qualifier used for backup-discrete profiles. Recommended is a revoked userid (not group id) without the GRPACC attribute.

DMS_SECURE_PARMLIB

Flag field that indicates if the site security setting for DMS PARMLIBs is turned on.

- If DMS PARMLIB=Y, the site has restricted the use of DMS PARMLIBs to a set of specific data set names using the DMS Security Parmlib feature. This flag is set in the load module ADSTS148 together with an authorized parmlib data set name.
- If DMS PARMLIB=N or the value is not specified, it indicates a major security loophole that permits any user to deactivate RACF processing in DMS, bypassing RACF security.

DMSSECURVOL

This DMS parameter indicates whether DMS is to use the RACF DASDVOL class. If set to 'Y' DMS first checks DASDVOL authority before it checks data set-level authority. If DASDVOL authority is granted, no further checks are performed.

DYNAMIC_CDT

Indicates if the dynamic class descriptor table (CDT) feature of RACF is active on the system. On systems not running RACF the field is missing.

EARLYVERIFY

This flag indicates whether JES is to call the system authorization facility (SAF) for jobs that do not qualify for userid propagation. If set to EARLYVERIFY=YES, JES verifies the user id, group, and password at job submission time. For JES2 3.1.3 and later, this flag is not tested and job processing occurs as if the value

was YES. The option indicated by this flag can be set by a SETROPTS JES(EARLYVERIFY) command. This field supports overtype.

EGN

Flag field that indicates if enhanced generic naming (EGN) is in effect due to a SETROPTS EGN command. This field supports overtype.

EIMREGISTRY

For z/OS 1.4 and z/OS 1.5, this field contains the name of the RACF registry of this system in the EIM domain. For those releases only, the value is set at IPL, or whenever SETROPTS EIMREGISTRY is issued. The value is obtained from the FACILITY profile IRR.PROXY.DEFAULTS.

On z/OS 1.6 and higher, RACF does no longer maintain an in-storage pointer to the registry name, and the EIMREGISTRY field is missing. It is the responsibility of the EIM registry application to obtain the EIM environment information (which includes the registry name) from the FACILITY profile.

ERASEONSCRATCH, EOS

This string indicates whether erase-on-scratch is in effect (due to a SETROPTS ERASE command). If in effect, data sets are physically erased when deleted or released for reuse. The ERASEONSCRATCH values and their meaning are documented in the following table. This field is only present on a RACF system.

ERASEONSCRATCH value	Meaning
All	All data sets are physically erased after delete (due to a SETROPTS ERASE(ALL) command)
Lvlnnn	Physical erasure is performed if the profile that protects the data set specifies ERASE or if the profile's security level is equal to or greater than the erase security level *nnn* as specified on the SETROPTS ERASE(SECLEVEL) command.
None	No data sets are physically erased after delete, even if the erase indicator in the data set profile is on as a result of a SETROPTS NOERASE command.
Profile	The erase indicator in the data set profile is used to determine whether the data set is physically erased after delete as a result of a SETROPTS ERASE(NOSECLEVEL) command.

Note that, when migrated or backed up data sets are scratched from HSM owned DASD volumes, the field HSMERASE determines if HSM actually performs the erasure requested by the profile.

ERASESECLEVEL, SECLEVELERASE

String value that indicates the security level at or above which all data sets are physically erased when deleted or released for reuse as a result of a SETROPTS ERASE(SECLEVEL) command. If the value is *None*, the ERASEONSCRATCH field determines erasure options. Otherwise, this field contains a number. This field is only present on a RACF system.

ESMNAME

Name of the active external security manager.

ESMLVL, ESMLEVEL

The release level of the active external security manager. For RACF, this field also contains IRRDPSDS (dynamic parse) APAR level, IRRTEMP1 (RACF templates) APAR level, and, if available, the numerical equivalents of release level and APAR level.

FORCE24, BELOW

This flag indicates whether all ACEEs reside below the 16 MB line (in 24-bit addressable memory). It is set if one or more exits reside below the 16 MB line.

GENANC_JOBCOUNT

This field is part of a repeat group. It shows the number of generic anchors that RACF maintains for jobs matching the associated JOBNAME value. This field can be specified using the RACF SET GENERICANCHOR command.

GENANC_JOBNAME

This field is part of a repeat group that shows the number of generic anchors RACF maintains for jobs matching the JOBNAME value. This field can be specified using a RACF SET GENERICANCHOR command. Job names with an (*) as the last character specify a set of similarly named jobs.

GENANC_SYSTEM_COUNT

Contains the number of generic anchors that RACF maintains for any job for which no applicable JOBNAME has been specified in a RACF SET GENERICANCHOR command.

GENERICOWNER, GENOWN

This flag indicates whether restrictions on the creation of generic profiles are in effect (due to a SETROPTS GENERICOWNER command). If set (GENERICOWNER=YES), users can only create a generic profile more specific than any existing profile covering the same generic resource if:

- The user has the SPECIAL attribute
- The user is the owner of the existing profile
- The profile is owned by a group and the user is group-SPECIAL in that group.
- The profile is owned by a user in a group and the current user is group-SPECIAL in that group.

This option does *not* apply to the class DATASET; for class DATASET, the CREATE authority determines who can create profiles. This field supports overtype. This field is only present on a RACF system.

GRPLIST, LISTGRP

Flag field that indicates if list-of-groups processing is in effect as a result of SETROPTS GRPLIST command. If set (GRPLIST=YES), user authority to a resource is not based only on the authority of the user's current connect group but also on the highest authority of all groups the user is connected to. This field supports overtype. This field is only present on a RACF system.

HISTORY, PWDHISTORY

This string indicates the number of previous passwords stored by RACF (due to a SETROPTS PASSWORD(HISTORY) command). If set to '**No**', no password history is kept; otherwise, it contains a number in the range 1 to 32. This field supports overtype.

HSMBACKUPPREFIX

This string indicates the prefix of the data set name HSM generates when it backs up a data set. If not set, HSM uses the userid specified in the HSM startup procedure.

This field is determined by the BACKUPPREFIX parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMERASE

Flag field that indicates ifHSM asks RACF for the erase status of the user data set when backed up or migrated data sets are scratched from HSM-owned DASD volumes. If this flag is not set (HSMERASE=NO) and the ERASEONSCRATCH field is set to erasure, this indicates a security exposure.

This field is determined by the ERASEONSCRATCH parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMJOBNAME

This repeated field contains the job names for identifying the DFSMShsm instances started on the system

HSMLEVEL, HSMLVL

String indicating the software level of HSM. This repeated field is reported once for every instance of DFSMShsmstarted on the system.

HSMMIGRATEPREFIX

This string indicates the prefix of the data set name HSM generates when it migrates a data set. If not set, HSM uses the userid specified in the HSM startup procedure.

This field is determined by the MIGRATEPREFIX parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMMULTITAPEVOL

Flag field that indicates if HSM uses more than one TAPEVOL profile to protect the volume pool. This flag is not used in recent HSM releases. This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMPROFILEBACKUP, HSMBACKUPPROFILE

This flag indicates whether HSM creates a backup RACF discrete profile when it backs up a cataloged RACF-indicated data set.

This field is determined by the PROFILEBACKUP parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMRACFIND

Flag field that indicates if RACF is to put RACF-indication on migrated and backed up data sets. Specify HSMRACFIND=YES unless all of the following conditions are met:

- RACF always-call is in effect.
- Generic profile checking is in effect.
- Generic profiles have been defined that cover the migration and backup qualifiers.

The value for the HSMRACFIND setting is determined by the RACFIND parameter of the HSM SETSYS command.

HSMRACFIND is a repeated field that is reported once for every instance of DFSMShsm started on the system.

HSMSMFRECNO

This field indicates the SMF record type used for HSM daily and volume statistics records; HSM function statistics have SMF record type HSMSMFRECNO+1. If "No", HSM does not write SMF records or HSM is not active on this system.

This field is determined by the SMF parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HSMTAPESECURITY

This field contains the DFSMShsm tape security setting, as described in the DFSMShsm diagnosis Reference, offset 437 in the MCVT.

HSMTAPESELVOL

Flag field that indicates if HSM is to allocate new tapes from its own pool or from the system scratch tapes.

This field is determined by the SELECTVOLUME parameter of the HSM SETSYS command.

This repeated field is reported once for every instance of DFSMShsm started on the system.

HWNAME

This string contains the hardware name.

IKJTSO

This string contains the current source for TSO parameters. It has the form IKJTSO**xx** if the source for TSO parameters is parmlib member IKJTSO**xx**; it is set to PARMLIB if the TSO options have been changed online by the PARMLIB command.

INACTIVE

This string indicates the number of days that a userid remains valid without being used (due to a SETROPTS INACTIVE command). If set to '**No**', users are never revoked because of lack of activity; otherwise, it contains a number in the range 1 to 255. This field is only present on a RACF system.

Note that inactive users are only revoked by RACF the next time user activity is attempted, for instance the next time the now inactive user tries to logon. Inactive users can be found using the CARLa script CKRLINAC. This field supports overtype.

INITSTATS

Flag field that indicates if RACF statistics are updated by RACINIT processing (due to a SETROPTS INITSTATS command). This field supports overtype.

INTERVAL, PWDINTERVAL

This string indicates the maximum number of days a password remains valid (due to a SETROPTS PASSWORD(INTERVAL) command). If set to '**No**', passwords never expire; otherwise, it contains a number in the range 1 to 254. This field supports overtype. This field is only present on a RACF system.

IODF_CONFIG_DATE

The date the active IODF configuration was last updated. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

IODF_CONFIG_ID

This string contains the name of the configuration selected from those defined in the IODF.

IODF_CONFIG_TIME

The time the active IODF configuration was last updated. This field can only be used for output, and not for SELECT/EXCLUDE processing.

IPLDATE

The date the system was last IPLed, in the format 'DD MMM YYYY'. For detailed instructions on how to use this field in SELECT/EXCLUDE specifications, see "Date fields" on page 903.

IPLDEV

This string indicates the device number of the IPL device. The value returned has four characters. The first character returned might be a blank if the value is a three-digit device number.

IPLPARM parameters

For further information on these variables, refer to the z/OS MVS Initialization and Tuning Reference, especially the section that documents the (system initialization parmlib member `IEASYS`*`xx`*. The effective parmlib specification at IPL time can be found in IPLPARM_LOAD; also check IPLPARM_PARMLIB_LOAD. Note that IEASYS00 is always processed first, followed by any `IEASYS`*`xx`* members with the suffixes documented in IPLPARM_SYSP These IEASYSxx members might override earlier parameter specifications. The parameter specifications might be updated several times during the IPL process. The last, and therefore the effective, parameter specification at IPL time is documented in the IPLPARM variables. Some parameters can be updated dynamically after IPL using system commands such as SET and SETPROG. The results from these actions are not shown in the IPLPARM variables.

IPLPARM_ALLOC

This string contains the list of suffixes passed at IPL time that specifies the names of the ALLOCxx parmlib members. These members describe installation defaults for allocation parameters. Value `00` indicates parmlib member ALLOC00. This setting can also be specified using the ALLOC parameter of parmlib member `IEASYS`*`xx`*.

IPLPARM_APF

Contains the suffix passed at IPL time that specifies the name of the `IEAAPF`*`xx`* parmlib member. This member contains authorized library names. Value `00`

indicates parmlib member IEAAPF00. This setting can also be specified using the APF parameter of parmlib member IEASYS*xx*.

IPLPARM_AUTOR
String field that contains the list of suffixes at IPL time that specify the names of the AUTOR*xx* parmlib members. These members contain the auto-reply policy for WTOR messages. This suffix is specified using the AUTOR parameter of parmlib member IEASYS*xx*.

IPLPARM_AXR

The IPLPARM_AXR field is a string field that contains the suffix that completed the name of the parmlib member AXR*xx* at system IPL. Parmlib member AXR*xx* contains system REXX parameters. (Value 00 indicates the parmlib member AXR00.) This suffix is specified using the AXR parameter of parmlib member IEASYS*xx*.

IPLPARM_CATALOG

This string contains a list of suffixes passed at system IPL that specify the names of IGGCAT*xx* parmlib members. These members can be used to define catalog system parameters. Value 00 indicates parmlib member IGGCAT00. This setting can also be specified by using the CATALOG parameter of parmlib member IEASYS*xx*.

IPLPARM_CEE

This string contains a list of suffixes passed at IPL time that specifies the names of the CEEPRMxx parmlib members. These members are used to provide default Language Environment run-time options for the system. Value 00 indicates parmlib member CEEPRM00). This setting can also be specified using the CEE parameter of parmlib member IEASYS*xx*.

IPLPARM_CLOCK

This string contains the parameters passed at IPL time that specify the name of the CLOCKxx parmlib member. This parmlib member indicates whether to prompt the operator to set the TOD clock during system initialization, specifies the time zone, and controls ETR usage. Value 00 indicates parmlib member CLOCK00.

This setting can also be specified using the CLOCK parameter of parmlib member IEASYS*xx*.

IPLPARM_CLPA

Flag field that indicates if the last IPL explicitly requested loading the LPA from the LPALST concatenation. This request is always occurs implicitly on a cold start. However, sometimes the explicit specification in an IEASYS*xx* member does not always show up. As a result, the value for IPLPARM_CLPA setting is shown as *YES* or blank by default, not as *NO*.

When IPLPARM_CLPA=YES, it also implies that the IPLPARM_CVIO value is *YES*, which means that previous VIO data set pages are purged.

The IPLPARM_CLPA setting can also be specified using the CLPA parameter of parmlib member IEASYS*xx*.

IPLPARM_CMB

This string contains the list of the I/O device class parameters passed at IPL time for which measurement data is collected (besides the DASD and tape device classes). This setting can also be specified via the CMB parameter of parmlib member IEASYS*xx*.

IPLPARM_CMD

This string contains a list of parameters passed at IPL time that specifies the names of the COMMND*xx* parmlib members. These members contain automatic operator commands to be issued during master scheduler initialization. Value `00` indicates parmlib member COMMND00.

This setting can also be specified using the CMD parameter of parmlib member IEASYSxx.

IPLPARM_CON

This string contains the suffix passed at IPL time that specifies the name of the CONSOLxx parmlib member. This member contains console, syslog and hardcopy definitions. Value `00` specifies parmlib member CONSOL00, The value NONE specifies that the IBM default values be used for the definitions so that message routing is determined by the IMSI values specified during initialization. Adding the NOJES3 keyword to the string allows JES2 functions incompatible with JES3 to operate successfully when JES3 is installed but not in use. If the string contains NOJES3 only, NONE is implied and the system uses the IBM default values. These settings can also be specified using the `CON` parameter of parmlib member `IEASYS`*`xx`*. Logically, this field contains the IPL specification, while the active setting is in `CON_CONSOL`. However, the `CON_CONSOL` parameter is not dynamic, the values are the same.

IPLPARM_COUPLE

This string contains the suffix passed at IPL time that specifies the name of the COUPLExx parmlib member. This member describes the sysplex environment for the initializing system. Value `00` indicates parmlib member COUPLE00.

This setting can also be specified using the COUPLE parameter of parmlib member `IEASYS`*`xx`*.

IPLPARM_CSA

This string contains the sizes of the virtual common service area (CSA) and extended common service area (ECSA) as specified at IPL time. The default unit for either size is 1 KB blocks.

This setting can also be specified using the CSA parameter of parmlib member `IEASYS`*`xx`*.

IPLPARM_CSCBLOC

This string indicates whether the CSCB control block chain is located above or below the 16 MB line as specified at IPL time.

This setting can also be specified using the CSCBLOC parameter of parmlib member IEASYSxx.

IPLPARM_CVIO

Flag field that indicates if the last IPL explicitly requested that all VIO data set pages be purged from auxiliary storage. This request is implicitly issued on a cold start. However, an explicit specification in an `IEASYS`*`xx`* member does not always show up. As a result, the value for `IPLPARM_CVIO` setting is shown as *`YES`* or blank by default, not as *`NO`*. The setting `IPLPARM_CVIO=YES` is implicitly specified by `IPLPARM_CLPA=`*`YES`*.

The `IPLPARM_CVIO` setting can also be specified using the `CVIO` parameter of parmlib member `IEASYS`*`xx`*.

IPLPARM_DEVSUP

This string contains a list of suffixes passed at IPL time that specifies the names of the DEVSUP*xx* parmlib members. These members specify the installation defaults for device support options. The value 00 indicates parmlib member DEVSUP00.

This setting can also be specified using the DEVSUP parameter of parmlib member IEASYS*xx*.

IPLPARM_DIAG

This string contains a list of suffixes passed at IPL time that specifies the names of the DIAGxx parmlib members. These members control the common storage tracking function and GFS tracing. Value 00 indicates parmlib member DIAG00.)

This setting can also be specified using the DIAG parameter of parmlib member IEASYS*xx*.

IPLPARM_DRMODE

Flag field that indicates if this system has been IPLed as part of a disaster recovery scenario. The setting can be specified via the DRMODE parameter of parmlib member IEASYS*xx*.

IPLPARM_DUMP

This string specifies whether cataloged SYS1.DUMPxx data sets on permanently resident volumes are to be made available on direct-access devices (DASD) or not (NO) at IPL time, and if so optionally a range for the *xx*-suffix, (especially notable in case of DASD shared between systems. The default range is SYS1.DUMP00 through SYS1.DUMP99.

This setting can also be specified using the DUMP parameter of parmlib member IEASYS*xx*.

IPLPARM_DUPLEX

This string contains the name of a paging data set to be used to hold a secondary copy of all common area system pages as specified at IPL time. It is only meaningful on a cold start. That is, if the CLPA parameter was specified or implied. This setting can be specified using the DUPLEX parameter of parmlib member IEASYS*xx*.

IPLPARM_EFFECTIVE

This string contains all effective IPL parameters separately available in the IPLPARM_<parameter> variables, plus possibly obsolete specifications or defaults. See also IPLPARM_OPERATOR. See the separate variables and/or the Initialization and Tuning Reference (section IEASYS*xx*) for further documentation.

IPLPARM_EXIT

This string contains a list of suffixes passed at IPL time that specifies the names of the EXITxx parmlib members. These members contain the entry points and names of allocation installation exits. Value 00 indicates parmlib member EXIT00. This setting can also be specified using the EXIT parameter of parmlib member IEASYS*xx*.

IPLPARM_FIX

This string contains a list of suffixes passed at IPL time that specifies the names of the IEAFIXxx parmlib members. These members contain names of modules to be placed in a fixed LPA that lasts for the duration of the IPL. Value 00 indicates

parmlib member IEAFIX00.) You can also specify the NOPROT keyword to indicate that the fixed LPA is not page-protected.

These settings can also be specified using the FIX parameter of parmlib member IEASYS*xx*. See also IPLPARM_MLPA.

IPLPARM_GRS

This string contains a keyword value indicating whether the system is to participate in a global resource serialization complex or not (NONE), and if so, how, as specified at IPL time.

This setting can also be specified using the GRS parameter of parmlib member IEASYS*xx*.

IPLPARM_GRSCNF

This string contains the suffix passed at IPL time that specifies the name of the GRSCNFxx parmlib member. This member contains essential configuration information for a system to participate in a global resource serialization complex. This specification is not used if GRS=NONE is present at IPL time, and might be absent if GRS=STAR is specified. If no suffix is specified, the value defaults to 00 to indicate parmlib member GRSCNF00.

This setting can also be specified using the GRSCNF parameter of parmlib member IEASYS*xx*.

IPLPARM_GRSRNL

This string contains a list of suffixes passed at IPL time that specifies the names of the GRSRNLxx parmlib members. These members contain the resource name lists (RNLs) to be used for global resource serialization. Value <pv>00</pv> indicates parmlib member GRSRNL00. You can also specify the EXCLUDE keyword to indicate no RNLs are to be used at all. This setting can also be specified using the GRSRNL parameter of parmlib member IEASYS*xx*.

IPLPARM_HVCOMMON

This string contains the size of the 64-bit common area. The value is expressed in G or T, meaning gigabyte and terabyte respectively. The default setting is 64 GB. This setting can also be specified using the HVCOMMON parameter of parmlib member IEASYS*xx*.

IPLPARM_HVSHARE

This string contains the amount of virtual storage that can be shared. The value is expressed in G, T, or P, meaning gigabyte, terabyte, and petabyte respectively. If the value equals '0' (without G, T, or P) the default setting of 510 TB is used. This setting can be specified using the HVSHARE parameter of parmlib member IEASYSxx.

IPLPARM_ICS

This string contains the suffix passed at IPL time that specifies the name of the IEAICSxx parmlib member. This member contains the installation control specification used by the system resources manager to assign performance groups. Value 00 indicates parmlib member IEAICS00. This setting can also be specified using the ICS parameter of parmlib member IEASYS*xx*.

IPLPARM_IKJTSO

This string contains the suffix passed at IPL time that specifies the name of the IKJTSOxx parmlib member . This member contains the TSO/E settings for the system. This setting can also be specified using the IKJTSO parameter of parmlib member IEASYSxx.

IPLPARM_ILMLIB

String that defines the data set for the IBM Tivoli License Compliance Manager (TLCM). The default ILMLIB data set is SYS1.ILMLIB.S&SYSNAME(-7:7). You can also specify NODATASET. See also the IPLPARM_ILMMODE keyword.

IPLPARM_ILMMODE

Text string that specifies the settings for the ILMMODE at IPL time. ILM is the IBM Tivoli License Compliance Manager. The available modes are FIRSTIPL, NORMAL, and EMERGENCY. These settings can also be specified using the ILMMODE parameter of parmlib member IEASYS*xx*. See also the IPLPARM_ILMLIB keyword.

IPLPARM_IOS

String that contains the suffix passed at IPL time. The suffix specifies the name of the IECIOS*xx* parmlib member. This member contains control statements for the I/O supervisor. Value 00 indicates parmlib member IECIOS00. This setting can also be specified using the IOS parameter of parmlib member IEASYS*xx*.

IPLPARM_IPS

This string contains the suffix passed at IPL time that specifies the name of the IEAIPSxx parmlib member. This member contains the installation performance specification to be used by the system resources manager. Value 00 indicates parmlib member IEAIPS00.

This setting can also be specified using the IPS parameter of parmlib member IEASYS*xx*.

IPLPARM_IXGCNF

This string contains a list of suffixes passed at system IPL that specify the names of the IXGCNF*xx* parmlib members. These members can be used to control tracing and monitor intervals for the z/OS system logger. Value 00 indicates parmlib member IXGCNF00. This setting can also be specified by using the IXGCNF parameter of parmlib member IEASYS*xx*.

IPLPARM_LFAREA

This string contains the amount of real storage to be made available for 1 MB pages. The value can be expressed as a percentage of all online real storage available at IPL time, or in M or G meaning megabyte and gigabyte respectively. The default is none, which means that no LFAREA is defined. This setting can also be specified using LFAREA parameter of parmlib member IEASYSxx.

IPLPARM_LICENSE

This text string specifies the setting for what operating system is licensed at IPL time , z/OS or z/OSe, for example. This setting can be specified using the LICENSE parameter of parmlib member IEASYS*xx*.

IPLPARM_LNK

This string contains a list of suffixes passed at IPL time that specifies the names of the LNKLST*xx*parmlib members. These members contain names of data sets to be concatenated to SYS1.LINKLIB to form the LNKLST concatenation. Value <pv>00</pv> indicates parmlib member LNKLST00. In addition to the names specified, SYS1.MIGLIB and SYS1.CSSLIB are concatenated. This specification is

ignored if you specify the LNKLST ACTIVATE statement in a PROG*xx* member. See the IPLPARM_PROG keyword description.

The PROG*xx* member can also specify alternates for the SYS1 data sets mentioned above. This setting can also be specified using the LNK parameter of parmlib member IEASYS*xx*.

IPLPARM_LNKAUTH

Flag field that indicates if the last IPL explicitly requested to treat all libraries in the LNKLST concatenation as APF-authorized when accessed as part of that concatenation, or only those named in the APF table (APFTAB).

This setting can also be specified using the LNKAUTH parameter of parmlib member IEASYS*xx*. Logically, this field contains the IPL specification, while the active setting is in the LNKAUTH parameter (without the prefix). However, the LNKAUTH parameter is not dynamic, so the values are the same.

IPLPARM_LOAD

Repeat group that lists the effective LOAD*xx* cards. This list does not contain filter cards HWNAME, LPARNAME, VMUSERID, and no cards unless selected by the filter cards. Furthermore, the PARMLIB cards differ from those in the LOAD*xx* member in the following ways:

- If a card with the default is added, the text string *Default* is shown as a comment behind the actual 72-character card.
- Volume serials like ****** and **MCAT** have been resolved. This is indicated by the text string *Volume from catalog*.

If a data set error occurs, the comment field includes the text string *Failed* followed by an indication of what operation failed: LOCATE, MOUNT, or OPEN.

IPLPARM_LOGCLS

This string contains the JES output class for the log data sets as specified at IPL time. A log data set is queued to this class when its limit has been reached. See 1448.

This setting can also be specified using the LOGCLS parameter of parmlib member IEASYS*xx*. Logically, this field contains the IPL specification when the active setting is in SYSLOG_CLASS. However, the SYSLOG_CLASS parameter is not dynamic, so the values are the same.

IPLPARM_LOGLMT

Indicates the maximum number of messages permitted for each log data set as specified at IPL time. When this limit is reached, the log data set is closed and queued to JES, and a new log data set is used. This value is also specified by the LOGLMT parameter of parmlib member IEASYS*xx*. The value must be a six-digit number with leading zeroes. Logically, this LOGLMT parameter contains the IPL specification, while the active setting is in SYSLOG_LIMIT parameter. However, the LOGLMT parameter is not dynamic, so the values are the same.

IPLPARM_LOGREC

String that specifies the logrec recording medium for error and environmental recording as specified at IPL time. The value is either the name of the data set for logging or one of the following reserved keywords:

- LOGSTREAM specifies that logging is directed to the sysplex-wide repository SYSPLEX.LOGREC.ALLRECS
- *IGNORE* specifies do not record.

The IPLPARM_LOGREC setting can also be specified by theLOGREC parameter of parmlib member of IEASYS*xx*.The logrec recording medium specification can also be altered by the SETLOGRC command.

IPLPARM_LPA

This string contains a list of suffixes passed at IPL time that specifies the names of the LPALST*xx* parmlib members. These members contain the names of the data sets to be concatenated to SYS1.LPALIB to form the LPALST concatenation. Value *00* indicates parmlib member LPALST00.) You can optionally specify an alternate data set for SYS1.LPALIB using the PROG*xx* parmlib member. This setting can also be specified using the LPA parameter of parmlib member IEASYS*xx*. See also the IPLPARM_PROG and IPLPARM_MLPA keywords.

IPLPARM_MAXCAD

This string contains the maximum number of SCOPE=COMMON data spaces as specified at IPL time. This setting can also be specified using the MAXCAD parameter of parmlib member IEASYS*xx*.

IPLPARM_MAXUSER

This string contains a value that is in principle the maximum number of concurrent jobs and started tasks as specified at IPL time. There are some exceptional conditions when the actual limit is higher: see IPLPARM_RSVNONR and IPLPARM_RSVSTRT. This setting can also be specified using the MAXUSER parameter of parmlib member IEASYS*xx*.

IPLPARM_MLPA

This string contains a list of suffixes passed at IPL time that specifies the names of the IEALPAxx parmlib members. These members contain names of modules to be added to the pageable LPA as an extension that lasts for the duration of the IPL. (Value 00 indicates parmlib member IEALPA00.) In addition, the NOPROT keyword can be present, in which case the extension is not page-protected. These settings can be specified using the MLPA parameter of parmlib member IEASYSxx. See also IPLPARM_FIX and IPLPARM_LPA.

IPLPARM_MSTRJCL, IPLPARM_MSTJCL

This string contains the suffix passed at IPL time that specifies the name of the MSTJCLxx parmlib member. This member contains the JCL used to start the master scheduler address space. Value <pv>00</pv> indicates parmlib member MSTJCL00. This setting can also be specified using the MSTRJCL parameter of parmlib member IEASYS*xx*. See also IPLPARM_MSTRJCL_LINKLIB.

IPLPARM_MSTRJCL_LINKLIB, IPLPARM_MSTJCL_LINKLIB

This flag indicates whether the master JCL was loaded from SYS1.LINKLIB. Normally, the MSTJCL suffix specifies the MSTJCL*xx* member in parmlib, but if the parmlib does not contain that member, the system checks whether link library has a module of that name, and then uses that. If the module cannot be found, the suffix 00 is tried. If that also fails, the operator is prompted to specify the member.

IPLPARM_NONVIO

This repeat group contains the list of local page data sets that have been excluded from direct VIO paging (as long as space is available elsewhere) at IPL time. This setting can also be specified using the NONVIO parameter of parmlib member IEASYSxx.

IPLPARM_NSYSLX

This string contains the number of system linkage indexes to reserve as specified at IPL time. This setting can be specified using the NSYSLX parameter of parmlib member IEASYS*xx*.

IPLPARM_OMVS

This string contains a list of suffixes passed at IPL time that specifies the names of the BPXPRMxx parmlib members. These members contain the OpenEdition MVS (OMVS) configuration specifications. Value 00 indicates parmlib member BPXPRM00). You can specify the keyword DEFAULT to have OMVS start in its minimum configuration mode. This setting can also be specified using the OMVS parameter of parmlib member IEASYS*xx*.

IPLPARM_OPERATOR

This string contains the operator-specified parameters, a subset of the effective IPL parameters. See IPLPARM_EFFECTIVE.

IPLPARM_OPI

Flag field that indicates if the operator was prompted for certain IPL parameters during the last IPL. This setting can also be specified using the OPI parameter of parmlib member IEASYS*xx*.

IPLPARM_OPT

This string contains the suffix passed at IPL time that specifies the name of the IEAOPTxx parmlib member. This member contains parameters for the system resources manager. Value 00 indicates parmlib member IEAOPT00. This setting can also be specified using the OPT parameter of parmlib member IEASYS*xx*.

IPLPARM_PAGE_OPER

This repeat group contains the list of page data sets added by the operator at IPL time. These are added to the page data sets specified in an active IEASYS*xx* parmlib member, until the next cold or quick start.

IPLPARM_PAGE_SYS

This repeat group contains the list of page data sets specified in an IEASYSxx parmlib member at IPL time. This setting can also be specified using the PAGE parameter of parmlib member IEASYS*xx*. If the operator wants to replace the specified data sets, he must specify an alternate IEASYSxx member with the SYSP parameter. To temporarily add Page data sets, the operator can enter a PAGE parameter at the operator prompt.

IPLPARM_PAGTOTL

This string contains a pair of values, the total number of page and swap data sets, as specified at IPL time. This setting can also be specified using the PAGTOTL parameter of parmlib member IEASYS*xx*.

IPLPARM_PAK

This string contains a list of suffixes passed at IPL time that specifies the names of the IEAPAKxx parmlib members. This member contains groups of names of modules in the LPALST concatenation that are processed together or in sequence. Value 00 indicates parmlib member IEAPAK00. This setting can also be specified using the PAK parameter of parmlib member IEASYS*xx*. For the LPALST concatenation, see IPLPARM_LPA.

IPLPARM_PARMLIB_LOAD

This flag indicates that the LOADxx member used contained at least one PARMLIB card at IPL time. If this is not the case, the master JCL is loaded from the IEFPARM DD statement concatenation (or, if this fails, from parmlib). See also IPLPARM_LOAD.

IPLPARM_PLEXCFG

String field that indicates if the system is only permitted to IPL into a certain type of configuration or not (ANY), and if so, which one, as in effect at IPL time. This setting can also be specified using the PLEXCFG parameter of parmlib member IEASYS*xx*.

IPLPARM_PRESCPU

Flag field that indicates if the system brought online all CPUs that were online at the time the IPL was initiated, without regard to the number of CPUs defined to be initially online in the logical partition profile. This setting can also be specified using the PRESCPU parameter of parmlib member IEASYS*xx*.

IPLPARM_PROD

This string contains a list of suffixes that completed at IPL time the names of the IFAPRDxx parmlib members. These members contain the enablement policy for products or product features that can be dynamically enabled under z/OS. Value 00 indicates parmlib member IFAPRD00.

This setting can also be specified using the PROD parameter of parmlib member IEASYS*xx*.

IPLPARM_PROG

This string contains a list of suffixes passed at IPL time that specifies the names of the PROGxx parmlib members. These members specify the format and contents of the APF-authorized library list, the use of exits and exit routines, the standard libraries for the LNKLST and LPALST concatenations, and optionally the LNKLSTxx parmlib members to be used, overriding the LNK parameter. Value 00 indicates parmlib member PROG00.

This setting can also be specified using the PROG parameter of parmlib member IEASYS*xx*.

IPLPARM_RDE

Flag field that indicates if the reliability data extractor feature was specified to be included at IPL time.

This setting can also be specified using the RDE parameter of parmlib member IEASYS*xx*.

IPLPARM_REAL

This string contains a number, the maximum amount of central storage, in 1 KB blocks, that can be allocated for concurrent ADDRSPC=REAL jobs, as specified at IPL time. This setting can also be specified using the REAL parameter of parmlib member IEASYSxx. A nonzero value is a concern, because it enables non-privileged users to run in a key in the 9-15 range, thereby allowing them to alter the contents of CSA, ECSA, SQA, or ESQA storage with this key.

IPLPARM_RER

Flag field that indicates if using the reduced error recovery routines for magnetic tapes was requested at IPL time. This specification is effective only if

the procedures are stated on the OPTCD parameter on a data definition (DD) statement or on the DCB macro. This setting can also be specified using the RER parameter of parmlib member IEASYS*xx*.

IPLPARM_RSU

This string contains the number of central storage increments to be made available for storage reconfiguration, as specified at IPL time. This setting can also be specified via the RSU parameter of parmlib member IEASYS*xx*.

IPLPARM_RSVNONR

This string contains the number of entries in the address space vector table that are to be reserved for replacing entries that are marked non-reusable, as specified at IPL time. This is used to increase the limit specified by the MAXUSER parameter under certain conditions. This setting can also be specified using the RSVNONR parameter of parmlib member IEASYS*xx*. See also IPLPARM_MAXUSER and IPLPARM_RSVSTRT.

IPLPARM_RSVSTRT

This string contains the number of entries in the address space vector table that are to be reserved for address spaces created in response to a START command, as specified at IPL time. This is used to increase the limit specified by the MAXUSER parameter under certain conditions. This setting can also be specified using the RSVSTRT parameter of parmlib member IEASYS*xx*. See also IPLPARM_MAXUSER and IPLPARM_RSVNONR.

IPLPARM_RTLS

This string contains the suffix that completed at IPL time the name of the CSVRTLxx parmlib member. This member contains the run-time library system configuration. Value 00 indicates parmlib member CSVRTL00. This setting can also be specified using the RTLS parameter of parmlib member IEASYS*xx*.

IPLPARM_SCH

This string contains a list of suffixes that completed at IPL time the names of the SCHEDxx parmlib members that contains the master scheduler parameters. Value 00 indicates parmlib member SCHED00. This setting can also be specified using the SCH parameter of parmlib member IEASYS*xx*.

IPLPARM_SMF

This string contains the suffix that completed at IPL time the name of the SMFPRMxx parmlib member. This member contains the SMF parameters. Value 00 indicates parmlib member SMFPRM00. This setting can also be specified using the SMF parameter of parmlib member IEASYS*xx*.

IPLPARM_SMS

This string contains the suffix that completed at IPL time the name of the IDGSMSxx parmlib member. This is the member from which SMS obtains its parameters when the system is initialized with partitioned data set extended (PDSE) support. Value 00 indicates parmlib member IDGSMS00. This setting can also be specified using the SMS parameter of parmlib member IEASYS*xx*.

IPLPARM_SQA

This string contains the (additional) sizes of the virtual system queue area (SQA) and extended system queue area (ESQA) as specified at IPL time. The default unit for either size is 64 KB blocks. This setting can also be specified using the SQA parameter of parmlib member IEASYSxx.

IPLPARM_SSN

This string contains a list of suffixes that completed at IPL time the names of the IEFSSNxx parmlib members. These members contain the information needed to define and initialize selected subsystems. Value 00 indicates parmlib member IEFSSN00.

This setting can also be specified using the SSN parameter of parmlib member IEASYS*xx*.

IPLPARM_SVC

This string contains a list of suffixes that completed at IPL time the names of the IEASVC*xx* parmlib members. These members contain the installation-defined SVCs. Value 00 indicates parmlib member IEASVC00.

This setting can also be specified via the SVC parameter of parmlib member IEASYS*xx*.

IPLPARM_SWAP

This repeat group contains the list of swap data sets specified at IPL time. This setting can also be specified using the SWAP parameter of parmlib member IEASYS*xx*. Note that SWAP works unlike PAGE just as most parameters do, the last specification entirely replaces a previous one. This parameter is no longer supported in z/OS 1.5 and higher, so this field is always missing on those systems.

IPLPARM_SYSNAME

This string contains the name of the system being initialized, as specified at IPL time. This setting can also be specified using the SYSNAME parameter of parmlib member IEASYS*xx*.

IPLPARM_SYSP

This string contains a list of suffixes that completed at IPL time the names of the additional IEASYSxx parmlib members. These members contain system initialization parameters. Value 01 indicates parmlib member IEASYS01. This setting cannot be specified in IEASYS*xx*, but it can be specified using the SYSP parameter at the operator prompt. Note that IEASYS00 is always processed first.

IPLPARM_UNI

This string contains the suffix that completed the name of the parmlib member CUNUNIxx at IPL time. The information stored in CUNUNIxx is used by the Unicode Conversion Services to activate a conversion environment, or delete an inactive conversion environment. This setting can also be specified using the UNI parameter of parmlib member IEASYS*xx*

IPLPARM_VAL

This string contains a list of suffixes that completed at IPL time the names of the parmlib members (VATLSTxx) that contain the volume attribute list. Value 00 indicates parmlib member VATLST00. This setting can also be specified using the VAL parameter of parmlib member IEASYS*xx*.

IPLPARM_VIODSN

This string contains either the name of the VSAM data set for holding information about journaled VIO data sets, or the reserved keyword IGNORE (do not record), as specified at IPL time. This setting can also be specified using the VIODSN parameter of parmlib member IEASYSxx.

IPLPARM_VRREGN

This string contains a number, the default amount of central storage, in 1 KB blocks, to be allocated for concurrent ADDRSPC=REAL jobs, as specified at IPL time. This setting can also be specified using the VRREGN parameter of parmlib member IEASYS*xx*.

IPLPARM_ZZ

The IPLPARM_ZZ flag field indicates whether the ZIIPZAAP system option (or ZZ for short) has been enabled for this system. At system IPL, the ZZ option determines whether the system can perform System z Application Assist Processor (zAAP) processing work using the System z Integrated Information Processor (zIIP) when zAAP processors are not available. This option is specified using the ZZ parameter of parmlib member IEASYSxx.

IPLTIME

The time the system was last IPLed, in the format 'HH:MM'. This field can only be used for output, and not for SELECT/EXCLUDE processing.

IPLVOL

This string contains the name of the IPL volume.

JES2LEVEL, JES2LVL

String indicating the software level of the JES2 or JES3 running as the primary subsystem, e.g. 'SP 4.3.0'.

Currently there is no field which shows whether JES2 or JES3 is the primary subsystem in NEWLIST TYPE=SYSTEM. However, this is reported in message CKR0132 and can also be seen in the subsystem report (NEWLIST TYPE=SUBSYS).

JES2NODE, NODE, NODENAME

This string contains the JES2 node name for the JES2 running as the primary subsystem.

JOBSTEPCAT

Flag field indicating if JOBCAT and STEPCAT DD statements are permitted in jobs. From z/OS 1.5 and up, these DD statements are not permitted in jobs. These DD statements can be enabled or disabled by issuing the following MVS operator commands:

```
MODIFY CATALOG,ENABLE(JOBSTEPCAT)
   MODIFY CATALOG,DISABLE(JOBSTEPCAT)
```

KERBLVL

Contains the value of the SETROPTS KERBLVL setting, indicating the level of Kerberos support present on the system. It controls the types of encryption that can be used when setting up a Kerberos connection.

This field supports overtype on z/OS V1R2 and later. This field is only present on a RACF system.

LNKAUTH

This flag field indicates if all libraries in the linklist are considered APF-authorized, or if only those libraries that are also in the APFlist are considered authorized. If LNKAUTH=YES, all libraries are considered authorized. This setting is also specified by the LNKAUTH parameter in parmlib member IEASYS*xx*.

Note: If set, the libraries in the linklist are only considered authorized when accessed as part of the linklist concatenation. When used in a user-specified STEPLIB, a linklist library is only authorized if it is also part of the APFlist. Logically, this field contains the active setting, while the IPL specification is in IPLPARM_LNKAUTH. However, the IPLPARM_LNKAUTH parameter is not a dynamic parameter, so the values are the same.

LOADPARM

System load parameters as entered on the machine console prior to IPL. Usually consists of IPL device (4 digits), IOC ID (2 digits) and nucleus ID (1 digit). On VM systems running MVS, the device number can differ.

LPAR

Name of the logical partition (LPAR). This is taken from the RMF control blocks and is only present on IBM machines and full compatibles.

LVL1PREF

This string indicates whether RACF protection is in effect for data sets that have single-qualifier names (due to a SETROPTS PREFIX command). If set, it contains a 1- to 8-character first qualifier prefixed to the data set name to get the internal (resource) name. If empty, RACF protection for single-qualifier data sets is not in effect (due to a SETROPTS NOPREFIX command). This field supports overtype.

MEMLIMIT

This field can be used to set an installation wide limit on the virtual storage above the 2 GB line. The default is 0, meaning that no address space can use virtual storage above the line. However, this is a soft limit so every job can override it.

MINCHANGE

This field indicates the minimal number of days that must pass between a user's password changes (due to a SETROPTS PASSWORD(MINCHANGE()) command.) If set to 'No', users can change their passwords more than once on the same day; otherwise, it contains a number in the range 1 to 254. This field supports overtype.

MIXEDCASE

Flag field that indicates if mixed passwords are used as a result of a SETROPTS PASSWORD(MIXEDCASE command. This field supports overtype.

MLACTIVE

This string indicates whether RACF requires security labels to be present on all jobs, all resources defined in USER and DATASET, and all classes defined in the Class Descriptor Table (CDT) that require a security label. It reflects an option set by a SETROPTS MLACTIVE command. The following table documents the MLACTIVE values, the corresponding SETROPTS commands, and their meanings.

MLACTIVE value	SETROPTS command	Meaning
No	SETROPTS NOMLACTIVE	Security labels are not required

MLACTIVE value	SETROPTS command	Meaning
Warning	SETROPTS MLACTIVE(WARNING)	RACF allows jobs without a security label access to resources that do not have a security label, but issues a warning
Yes/Fail	SETROPTS MLACTIVE(FAILURES)	Security labels are required in all normal cases. Privileged started tasks and SPECIAL users are permitted to make requests as long as data is not declassified.
n/a	-	RACF version before 1.9

Classes in the Class Descriptor Table (CDT) that require a security label can be found using the SECLABEL field of NEWLIST TYPE=CLASS. This field supports overtype.

MLALEVEL

The multi-alias level, for example, the number of qualifiers used to look for a user catalog alias pointer in the master catalog.

MLQUIET

Flag field that indicates ifRACF is to keep the system in a tranquil state (due to a SETROPTS MLQUIET command). If set (MLQUIET=YES), only started procedures, console operators, or SPECIAL users are able to logon, start new jobs, or access resources. This field supports overtype.

MLS

This string indicates whether RACF prevents users from declassifying data in a system using security labels. It reflects an option set by a SETROPTS MLS command. The following table documents the MLS values, the corresponding SETROPTS commands, and their meanings.

MLS value	SETROPTS command	Meaning
No	SETROPTS NOMLS	Users are permitted to declassify data
Warning	SETROPTS MLS(WARNING)	Users are permitted to declassify data, but any such action generates a warning message.
Yes/Fail	SETROPTS MLS(FAILURES)	Users are not permitted to declassify data
n/a	-	RACF version before 1.9

This field supports overtype.

MLSTABLE

Flag field that indicates if the system has stabilized security labels (due to a SETROPTS MLSTABLE command). If set (MLSTABLE=YES), security labels can only be altered ifMLQUIET is in effect. This field supports overtype. This field is only present on a RACF system.

MODELGDG

Flag field that indicates if Generation Data Group (GDG) modeling is in effect (due to a SETROPTS MODEL(GDG) command). If set (MODELGDG=YES), the GDG base name, not the GDG generation name, is used to find the data set profile for the data set. This field supports overtype. This field is only present on a RACF system.

MODELGROUP

Flag field that indicates if group modeling is in effect (due to a SETROPTS MODEL(GROUP) command). If set (MODELGROUP=YES), RACF uses a model profile to complete new group-named data set profiles. This field supports overtype.

MODELUSER

Flag field that indicates if user modeling is in effect (due to a SETROPTS MODEL(USER) command). If set (MODELUSER=YES), RACF uses a model profile to complete new data set profiles named with the user ID. This field supports overtype.

MVSIOCID

IO configuration ID selected at IPL. The value '**xx**' indicates that the MVSCP IO configuration data set loaded was taken from SYS1.NUCLEUS members IEANCTxx IOSIITxx, IEFEDTxx, and IOSUCBxx.

MVSLEVEL, MVSLVL

String indicating the software level of MVS, e.g. 'SP4.3.0'.

NJEUSERID

This string indicates the userid to be used for SYSOUT or network jobs that enter the system without an RTOKEN or UTOKEN value. The string value cannot be set to a userid defined in the RACF database. This field supports overtype.

NOADDCREATOR

Flag field that indicates if the system has to suppress the ALTER permit added by default to each newly created profile for the userid of the creator. This field supports overtype. This field is only present on a RACF system.

NODUP

Flag field that indicates if duplicate data set names are permitted. Duplicate data set names are two data sets that both have discrete profiles but reside on different volumes. If set `NODUP=YES`, duplicate data set names are not allowed. The `NODUP` keyword is only supported on RACF systems.

Note: This flag reflects an option that can only be set through module ICHSECOP, not using the SETROPTS command.

OPERAUDIT

Flag field that indicates ifRACF is logging all actions permitted only because a user has the `OPERATIONS` or `group-OPERATIONS` attribute.

The `OPERAUDIT` keyword reflects an option set by the `SETROPTS OPERAUDIT` command. This field supports overtype.

OSLVL

This field returns the version and release of the operating system indicated by the OSNAME field.

OSNAME

This field returns the popular name of the operating system. The version is indicated by the OSLVL field. Also the vendor can be filled in (field OSVENDOR) if the operating system supports that field as a variable.

OSVENDOR

This field returns the company name of the operating system vendor indicated by the OSNAME field if the operating system supports this field as a variable. Otherwise it is blank.

PCMODE

String indicating the mode of RACF program control (as set using the APPLDATA of FACILITY profile IRR.PGMSECURITY). The mode can be 'Basic', 'EnhWarn' or 'Enhanced'. This feature is available in z/OS 1.4 and higher. RACF releases before z/OS 1.4 run in Basic mode.

PRIMARY_LANGUAGE

This field indicates the RACF primary language setting as set by SETROPTR LANGUAGE(PRIMARY()).

PROTECTALL

This string indicates whether RACF protect-all processing is active (due to a SETROPTS PROTECTALL command). The table below documents the PROTECTALL values, the corresponding SETROPTS commands, and their meanings

PROTECTALL value	SETROPTS command	Meaning
No	SETROPTS NOPROTECTALL	Users can access and create data sets that are not RACF-protected
Warning	SETROPTS PROTECTALL(WARNING)	Users can access and create data sets that are not RACF-protected, but any such action results in a warning
Yes/Fail	SETROPTS PROTECTALL(FAILURES)	Normal users are not permitted to access or create data sets that are not RACF-protected. Privileged started tasks and SPECIAL users are allowed to do so, but any such action generates a warning message.

This field supports overtype.

PWDRULE1

This string displays RACF password rule 1. RACF supports 8 different password rules, of which any one can be active or inactive as a result of a SETROPTS PASSWORD(RULE)) command. If active, the password rule is of the form '**Length(min:max) Pattern**' or '**Length(max) Pattern**'. The Pattern is a string of **max** characters indicating what characters are valid at that position; the following table documents the possible character values and their meaning.

Pattern character	Meaning
*	Any character
$	National
A	Alphabetic
C	Consonant
c	Mixed consonant
L	Alphanumeric
m	Mixed numeric
N	Numeric
V	Vowel
v	Mixed vowel
W	No vowel

When multiple password rules are active, RACF attempts to match a new password to any active rules but does not require matching all active rules. As a result, RACF permits a password that is accepted by one rule but not another.

PWDRULE2

This string displays RACF password rule 2. See the PWDRULE1 field.

PWDRULE3

This string displays RACF password rule 3. See the PWDRULE1 field.

PWDRULE4

This string displays RACF password rule 4. See the PWDRULE1 field.

PWDRULE5

This string displays RACF password rule 5. See the PWDRULE1 field.

PWDRULE6

This string displays RACF password rule 6. See the PWDRULE1 field.

PWDRULE7

This string displays RACF password rule 7. See the PWDRULE1 field.

PWDRULE8

This string displays RACF password rule 8. See the PWDRULE1 field.

RACF_AUTOAPPL

This flag field indicates whether RRSF automatically propagates application updates to the RACF database to remote nodes.

You can use the RACF SET AUTOAPPL operator command to specify the application updates options. This command needs to be repeated after each IPL. Therefore, it is normally incorporated in parmlib member IRROPTxx.

RACF_AUTODIRECT

This flag field indicates whether RRSF automatically propagates RACF commands to remote nodes.

You can use the RACF SET AUTODIRECT operator command to specify the automatic command direction options. This command needs to be repeated after each IPL. Therefore, it is normally incorporated in parmlib member IRROPTxx.

RACF_AUTOPWD

This flag field indicates whether RRSF automatically propagates password updates to remote nodes.

You can use the RACF SET AUTOPWD operator command to specify the automatic password direction options. This command needs to be repeated after each IPL. Therefore, it is normally incorporated in parmlib member IRROPTxx.

RACF_JESNODE

Specifies the JES node that is the destination for output that is redirected when the RRSFLIST data set is unusable.

RACF_MLFSOBJ

This string indicates whether RACF requires security labels for files and directories. When the SECLABEL class is active, and MLFSOBJ is active, access to files and directories without security labels is denied except by trusted or privileged started tasks. Since HFS file systems do not fully support security labels (except in read-only mode), conversion to zFS file systems is advisable before turning on this option. This field reflects the option set by a SETROPTS MLFSOBJ(ACTIVE | INACTIVE) command. This field supports overtype.

RACF_MLIPCOBJ

This string indicates whether RACF requires security labels for interprocess communications. When the SECLABEL class is active, and MLIPCOBJ is active, access to semaphores, message queues and shared memory without associated security labels is denied except by trusted or privileged started tasks. This field reflects the option set by a SETROPTS MLIPCOBJ(ACTIVE | INACTIVE) command. This field supports overtype.

RACF_MLNAMES

This string indicates whether the RACF name hiding function is in effect. This function has the following effects:

- Users cannot view the names of z/OS UNIX files and directories that their current security label does not give them authority to read.
- Users cannot view the names of data sets that a mandatory access check followed by a discretionary access check does not allow them to read.
- Users listing catalogs or directories cannot see the names of resources that they cannot currently read.
- Users cannot read a VTOC directly, unless they have been given authorization to the profile in the FACILITY class that protects the VTOC.

This field reflects the option set by a SETROPTS (NO)MLNAMES command. This field supports overtype.

RACF_PWSYNC

This flag field indicates whether RRSF honors the peer-to-peer password synchronization requested by the RACLINK command.

You can use the RACF SET PWSYNC operator command to specify the password synchronization options. This command needs to be repeated after each IPL. Therefore, it is normally incorporated in parmlib member IRROPTxx.

RACF_SECLBYSYSTEM

String that indicates if RACF permits security labels to be activated on a system image basis. When SECLBYSYSTEM is active, the SMF ID values specified in the member list of the profiles in the SECLABEL class determine whether or not

the security label is valid for each system. Security labels that are not valid for a system are considered inactive and cannot be used or listed by users without SPECIAL or AUDITOR on that system. This field reflects the option set by a SETROPTS (NO)SECLBYSYSTEM command. This field supports overtype.

RACF_SUBSYS_PREFIX

The command prefix for routing commands to the RACF subsystem on this system.

RACFACT

Flag field that indicates if RACF is active as a result of the RVARY ACTIVE command.

RACFDBLEVEL

String indicating the template level of the RACF database, for example, 'OA03853 00000010.00000010'.

RACFLEVEL, RACFLVL

A string field that represents the software release level, IRRDPSDS (dynamic parse) APAR level, and IRRTEMP1 (RACF templates) APAR level, as follows:

```
'HRF7730 HRF7730 HRF7730 00000064.00000010'
```

If a CKFREEZE data set produced by earlier versions of zSecure Collect program (CKFCOLL) is used as input, the format is as follows:

```
 '7.7.30  HRF7730 HRF7730 00000064.00000010'
```

This field is often tested by other products.

RACFLOCALNODE

This field returns the node name used by the RACF Remote Sharing Facility (RRSF) for the current system. It is only filled in if a CKFREEZE file of an APF-authorized run of zSecure Collect is being used.

You can use the RACF TARGET LOCAL operator command to specify the local node. This command needs to be repeated after each IPL. Therefore, it is normally incorporated in parmlib member IRROPTxx.

REALDSN

Flag field that indicates if RACF logging uses the real data set name (REALDSN=YES) or the naming-conventions name (REALDSN=NO) for logging purposes. It reflects an option set by the SETROPTS REALDSN command. This field supports overtype.

REFRPROT

This flag returns the status of the REFRPROT option which determines whether refreshable modules from non-APF libraries (REFR modules) are protected from modification. The following values can be returned:

Yes
Indicates that the REFRPROT option is enabled and REFR modules are protected from modification by loading them into Key 0 storage, and page protecting the full pages. This means the modules cannot be modified by key 8 (user key) programs. This is both a RAS (Reliability/Availability/Serviceability) advantage and a minor security advantage. However, setting REFRPROT might cause undesirable side effects for some programs.

No
Indicates that the NOREFRPROT option is enabled and REFR programs are not protected. This is the default setting for this option.

" " blank
Indicates that the REFRPROT option is not available. This option is only available on systems running z/OS version 1.9 and later versions.

The REFRPROT option can be set using the MVS command SETPROG or by specification in the PROGxx member of PARMLIB. For more information, see the *z/OS V1R9.0 MVS Initialization and Tuning Reference*

RETPD

This string specifies the RACF security retention period for tape data sets (due to a SETROPTS RETPD command). It is set to a number in the range 0 to 65533 for a tape data set that expires, and to 99999 for a tape data set that never expires. This field supports overtype.

REVOKE, PWDREVOKE

This string indicates the maximum number of consecutive invalid password attempts before a userid is revoked on the next invalid attempt (due to a SETROPTS PASSWORD(REVOKE) command). If set to '**No**', userids are never revoked because of invalid password attempts; otherwise, it contains a number in the range 1 to 254.

Notes: a REVOKE value of 5 means a userid is revoked at the *sixth* (not fifth) consecutive invalid password attempt. SPECIAL users are not revoked automatically after too many invalid password attempts; instead, console message ICH301I is issued, and the operator must decide whether or not to revoke the SPECIAL user. This field supports overtype. This field is only present on a RACF system.

RMFLEVEL, RMFLVL

String indicating the software level of RMF. If RMF is inactive, the *Inactive* is returned. If RMF active but zSecure Collect did not have sufficient authorization to collect the release level, the *Active* value is returned.

RVARYSTATUSPWSET

Flag field that indicates if the password for RVARY STATUS has been changed from the default value.

RVARYSWITCHPWSET

Flag field that indicates if the password for RVARY SWITCH has been changed from the default value.

SAUDIT

Flag field that indicates if RACF is logging all commands issued by users having the SPECIAL or group-SPECIAL attribute. It reflects an option set by the SETROPTS SAUDIT command. This field supports overtype.

SECLABELAUDIT

Flag field that indicates if security label auditing is in effect (due to a SETROPTS SECLABELAUDIT command). If set (SECLABELAUDIT=YES), RACF uses the security label's auditing options in addition to the profile's auditing options for all access attempts. If no auditing options are set on the security label's profile, this option has no effect. This field supports overtype.

SECLABELCONTROL

Flag field that indicates if security label control is in effect (due to a SETROPTS SECLABELCONTROL command). If you specify SECLABELCONTROL=YES, only the following users are permitted to use the SECLABEL keyword of RACF commands:

- SPECIAL users (all RACF commands)
- group-SPECIAL users ADDUSER and ALTUSER commands.

If the SECLABELCONTROL keyword is not set, all users with at least READ authority on the SECLABEL class can change profiles with this SECLABEL. This field supports overtype.

SECLEVELAUDIT

This string indicates whether security level auditing is in effect (due to a SETROPTS SECLEVELAUDIT command). If set to '**None**', auditing is not based on security levels; otherwise, it specifies the security level above which all access attempts are audited. This field supports overtype. This field is only present on a RACF system.

SECONDARY_LANGUAGE

This field indicates the RACF secondary language setting as set by SETROPTR LANGUAGE(SECONDARY()).

SECURPASS_SMF_LOG

Flag field that indicates ifProginet's SecurPass logging is active.

SECURPASS_SMF_RECNO

Contains the SMF record type written by the Proginet SecurPass application.

SESSIONINTERVAL, SESSINT

This string specifies the maximum session key interval that can be specified by RDEFINE or RALTER. It is set to a value in the range 1 to 32767 if session keys expire (SETROPTS SESSIONINTERVAL command) to '**None**' if no limit is set (due to a SETROPTS NOSESSIONINTERVAL command). This field supports overtype. This field is only present on a RACF system.

SMF_FLOOD_CONTROL

Indicates if a system has SMF flood detection. If SMF_FLOOD_CONTROL=Y, the SMF_FLOODPOL field contains the SMF flood policy records for SMF flood detection on the specified system.

SMF_FLOODPOL

Contains the SMF flood policy records for a given system if flood detection is active. The policy record for each unique set of SMF record types on the system is represented as a separate entry as shown in the following example.

```
FLOODPOL(TYPE(4,5),INTVLTIME(50),ENDINTVL(100),RECTHRESH(1000),
MAXHIGHINTS(10),ACTION(DROP))
```

FLOODPOL(ffff)

Specifies the flood control filter. The following parameters must be specified in the filter.

TYPE({*aa,bb*}|{*aa,bb:zz*}|{*aa,bb:zz,...*})

Numeric value in the range 0 - 255 that specifies the SMF record types that the filter applies to.

RECTHRESH(*xxxx*)

Numeric value in the range 1- 9999 that specifies the number of records permitted in an interval for a given filter.

INTVLTIME(*ssss*)
Numeric value in the range 1- 9999 that specifies the minimum amount of time that it can take to match the filter, measured in tenths of a second.

ENDINTVL(*ssss*)
Numeric value in the range 1 - 9999 that specifies the amount of time that the filter takes after the `recthreshold` is reached to determine a flood has ended, measured in tenths of a second.

MAXHIGHINTS(*xxxx*)
Numeric value in the range 1 - 9999 that specifies the number of intervals that must occur at or exceeding the flooding rate before action is taken.

ACTION({MSG|DROP})
Specifies the action to be taken when the `MAXHIGHINTS` threshold has been reached for the number of intervals at the specified flooding rate.

Table 556. Action to take when flood detection threshold has been exceeded

Action	Description
MSG	Issue warning message `IFA780A` at the start of the flood. Issue message `IFA781I` when the flooding has stopped.
DROP	Issue message `IFA782A` when the flood starts and also begin dropping records. When flooding ends, issue message `IFA783I` with the number of records dropped. Any attempts to write a record with the `SMFEWTM` or `SMFWTM` macro result in a return code *xx*. For information on the `SEFEWTM` and `SEFWTM` macros, , see the *z/OS MVS System Management Facilities* (SMF) documentation.

SMF17TEMP

Flag field that indicates if information for SMF record type 17 (Scratch Data Set Status) is to be collected for temporary data sets. It reflects the REC parameter in parmlib member SMFPRMxx. If set (SMF17TEMP=YES/REC=ALL), SMF record type 17 is written for both temporary data sets and non-temporary data sets; if not set (SMF17TEMP=NO/REC=PERM), SMF record type 17 is only written for non-temporary data sets.

SMF23INTERVAL, SMFSTATUS

This string indicates the amount of real time between creations of SMF record type 23 (SMF Statistics). It reflects the STATUS parameter in parmlib member SMFPRMxx. The SMF23INTERVAL field has the format 'HH:MM:SS' indicating hours, minutes, and seconds; an empty string indicates no status records are created.

SMFACTIVE

Flag field that indicates if SMF recording is active. It reflects the ACTIVE parameter in parmlib member SMFPRMxx. If set (SMFACTIVE=YES), SMF recording is active.

As an alternative to this field, you can consider using the SMFRECORDING field which also imparts the information whether SMF goes to data set or log stream. However, SMFACTIVE is a flag format field, while SMFRECORDING is a character field

SMFDS_ACTIVE

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_xx). Each repeat group entry describes one data

set. Flag field that indicates if the data set is in use (SMFDS_ACTIVE=YES) or not. (This flag describes the active data set at the time the CKFREEZE file was made.)

SMFDS_BLOCKS

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_). Each repeat group entry describes one data set. This field describes the number of blocks in the data set.

SMFDS_FILLED

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_). Each repeat group entry describes one data set. This field describes the percentage the data set is filled (in use), e.g. 75 if the data set is three-quarter full. (This number describes the data set at the time the CKFREEZE file was made.)

SMFDS_NAME

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_). Each repeat group entry describes one data set. This field describes the data set name, for example SYS1.MAN1.

SMFDS_SIZE

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_). Each repeat group entry describes one data set. This field describes the size of the data set in kilobytes.

SMFDS_VOL

This field is part of a repeat group describing the SMF recording data sets (all these fields start with SMFDS_). Each repeat group entry describes one data set. This field describes the data set volume.

SMFDUMPABNDRETRY

Flag field that indicates if the SMF dump program attempts to recover if an ABEND occurs. It reflects the DUMPABND parameter in parmlib member SMFPRM*xx*. If SMFDUMPABNDRETRY = YES, the SMF dump program attempts to recover from abends and to continue processing. If SMFDUMPABNDRETRY = *NO*, the SMF dump program terminates on an ABEND event.

SMFJWT

String value that indicates the maximum amount of real time that a job or TSO/E user is permitted to wait continuously before the time limit exit IEFUTL is entered.

This keyword reflects the JWT parameter in parmlib member SMFPRM*xx*. The SMFJWT field has the format 'HH:MM' indicating hours and minutes. If the IEFUTL exit is absent or is not in the exit list for the SMF subsystem, or if the exit does not take any action, a 522 ABEND results.

SMFLASTDSHALT, LASTDSHALT

This flag indicates the system action specified when the last available SMF data set has been filled and no more data sets are available for SMF use. It reflects the LASTDS parameter in parmlib member SMFPRMxx. If set (SMFLASTDSHALT=YES), the system enters a restartable wait state when the last SMF data set is filled; if not set (SMFLASTDSHALT=NO), the system issues a message and continues processing.

SMFLS_ACTIVE

A flag indicating whether the log stream is active or not. Active means SMF records are being directed to it.

SMFLS_BEING_CLEANED

A flag indicating that the system is in the process of removing records from the log stream or removing the log stream, but it still contains data. The field is part of the SMFLS_NAME repeat group.

SMFLS_BUFFERSIZE

The log stream buffer size in kilobytes. Output length is 7. The field is part of the SMFLS_NAME repeat group.

SMFLS_CONNECTED

Indicates that the log stream is connected and records can be written to it. Usually, the log stream status is also active. The exception is during the short period that elapses when an `SET SMF` command is in the process of removing the logstream.

The `SMFLS_CONNECTED` field is part of the `SMFLS_NAME` repeat group.

SMFLS_DEFAULT

A flag indicating whether this is the default SMF log stream or not. The default SMF log stream is the stream where records go that have not been redirected to other streams. The field is part of the SMFLS_NAME repeat group.

SMFLS_NAME

A repeating field of SMF log stream names. The default and maximum useful output length is 26. The field is part of the SMFLS_NAME repeat group that also contains SMFLS_SUMMARY, SMFLS_BUFFERSIZE, SMFLS_WRITETOD, SMFLS_DEFAULT, SMFLS_ACTIVE, SMFLS_BEING_CLEANED, and SMFLS_CONNECTED.

SMFLS_SUMMARY

A repeating field describing SMF log stream recording activity. It shows which SMF record types are being written to this log stream. This field has output length 255, so it is wise to put it as the last field of a line. The field is part of the SMFLS_NAME repeat group.

SMFLS_WRITE_TOD

Date and time stamp of the last write to an SMF log stream. Default output length is 15. The field is part of the SMFLS_NAME repeat group.

SMFMAXDORM, MAXDORM

This string indicates the amount of real time that SMF data can be buffered before being written to a recording data set. It reflects the MAXDORM parameter in parmlib member SMFPRMxx. The SMFMAXDORM field has the format 'MM:SS' indicating minutes and seconds; the value ' **none**' indicates data remains in the buffer until the buffer is full.

SMFNOBUFFSHALT, NOBUFFSHALT

This flag indicates the system action specified when the SMF address space runs out of buffer space. It reflects the NOBUFFS parameter in parmlib member SMFPRMxx. If set (SMFNOBUFFSHALT=YES), the system enters a restartable wait state when the SMF address space runs out of buffer space; no SMF data is lost. If not set (SMFNOBUFFSHALT=NO), the system issues a message and

continue processing; SMF data is lost until buffer storage is available again (in this case, an SMF type 7 record is written when buffer space is next available).

SMFPRM

This string contains the current source used for SMF parameters. It is set to blanks if the default parmlib member SMFPRMxx was used, and it is set to **xx** if the SET SMF command was used to specify a new parmlib member SMFPRM**xx**.

SMFRECORDING

A text field that shows one of the following:

OFF
Indicates that SMF recording is not active.

DATASET
Indicates that SMF recording is active and logging to data sets.

LOGSTRM
Indicates that SMF recording is active and logging to log streams.

This field can be a replacement for the SMFACTIVE setting, but that setting has a flag format. The output length is seven.

SMSLEVEL, SMSLVL

String indicating the software level of SMS and the products licensed in SMS. It has the format `DFSMSv.r.m dss hsm rmm '`; the product identifiers `DSS, HSM` and `RMM` are only returned if the product was licensed.

SYSCLONE

This is a shorthand version of the system name. Maximum length: 2 characters.

SYSLOG_ACTIVE

This flag field indicates that syslog is active.

SYSLOG_CLASS

The name of the JES output class used for the log data sets. A log data set is queued to this class when its limit has been reached, see the SYSLOG_LIMIT field. This value is specified in the `LOGCLS` parameter of parmlib member `IEASYS`*xx*. Logically, this field contains the active setting when the IPL specification is in `IPLPARM_LOGCLS`. However, the `SYSLOG_CLASS` parameter is not dynamic, so the values are the same.

SYSLOG_COMMANDS

This flag field indicates whether the hard copy command log has been set to SYSLOG using a VARY SYSLOG,HARDCPY command. If set, hard copy logging of commands is done to the system log.

SYSLOG_LIMIT

The maximum number of messages permitted for each log data set. When this limit is reached, the log data set is closed and queued to JES, and a new log data set is to be used. This value is specified in the `LOGLMT` parameter of parmlib member `IEASYS`*xx*.Logically, this field contains the active setting, while the IPL specification is in IPLPARM_LOGLMT. However, the `SYSLOG_LIMIT` parameter is not dynamic, so the values are the same.

SYSNAME

The system name as shown in the CVT, originating from the SYSNAME parameter in an IEASYS*xx* PARMLIB member. This value might be the same as the SMF ID retuned in the SYSTEM field.

SYSPERCENT

(not implemented, currently empty)

SYSPLEX

The sysplex name.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system ID. The field length is 8 characters to cater to VM systems.

TAPEDSN

Flag field that indicates if tape data set protection is in effect (due to a SETROPTS TAPEDSN command). If set (TAPEDSN=YES), RACF can protect tape data sets as well as tape volumes. This field supports overtype.

TAPEVOL

Flag field that indicates if the TAPEVOL class is active.

If TAPEVOL is inactive, RACF is not able to guarantee the integrity of tape volumes. Even if TAPEDSN is active, and even if you have a tape management system that assures 44 character data set name integrity (a tape only physically contains the last 17 in its data set header labels), it is still possible to circumvent security because of the fact that there is no protection between data sets on one tape. If you have access to one data set on a tape, you can use a non-APF-authorized program to access information of *all* data sets on the tape. So if you have TAPEVOL inactive, anyone can add an empty data set to that tape (unless it is completely full), and then access the other data sets.

The only way a tape management system can prevent this is either: always checking access to the tape based on the first data set on the tape or: prevent multiple data sets on a tape.

Another protection that is inactive if TAPEVOL is off, is the protection against Bypass Label Processing (BLP). If TAPEVOL is off, no RACHECKS are done by DFP on the FACILITY profile ICHBLP.

TCPIPPROC

This repeated field contains a list of the procedure names for TCP/IP procedures found in the TCP/IP stack.

TCPIPVERS

This repeated field contains a list of the version numbers of all TCP/IP procedures found in the TCP/IP stack.

TEMPDSFORMAT_UNIQUE

Flag field that indicates if the system generates unique data set names for temporary data sets that include `&&label` as the specified data set name, `DSN=&&mydsn` for example. The field value is based on the setting for the `ALLOCxx` `PARMLIB` option `TEMPDSFORMAT(`*`INCLUDELABEL`*`|`*`UNIQUE`*`)`. This field can have the following values.

YES. Indicates that `TEMPDSFORMAT=UNIQUE` is set. The system generates unique names with the following naming pattern:

SYSddddd.Thhmmss.jobname.RA000.Rggxxxxx form. This setting reduces the number of allocation failures caused by the system creating temporary data sets with the same name.

NO. Default value. Indicates that TEMPDSFORMAT= INCLUDELABEL is set. The system generates names in the legacy format which includes the &&dsname label. These names might not be unique.

blank. The TEMPDSFORMAT parameter is only supported for MVS V1R12 or later. For files defined on systems running earlier MVS releases, the field is blank.

TERMINAL

Flag field that indicates if the TERMINAL class is active (due to a SETROPTS CLASSACT(TERMINAL) command). This field is only present on a RACF system.

TERMUACC

This string indicates the default universal access authority associated with undefined terminals (due to a SETROPTS TERMINAL command). It can have the values 'NONE' and 'READ'. This field supports overtype. This field is only present on a RACF system.

TIMEZONE

This field indicates the systems time zone, in the format '**+** HH:MM' or '**-** HH:MM' indicating time relative to GMT. This field can only be used for output, not for SELECT/EXCLUDE processing.

TSOACBPW

This flag field indicates whether the TSO ACB password is present on the system. The password can be set with the ACBPW option in PARMLIB member TSOKEYxx. If a password is specified on the PRTCT parameter of VTAM's APPL definition statement from TSO/VTAM ACBs, then ACBPW must have been specified.

TSOCONFTXT

This field shows whether TSO/VTAM buffers are confidential. The data in the VTAM buffers is overwritten with zeros immediately after the data has been sent to the terminal. This setting also indicates that the buffer content cannot be traced. This option setting can be requested with the CONFTXT option in PARMLIB member TSOKEYxx.

TSOLEVEL, TSOLVL

String indicating the software level of TSO.

TSORECONLIM

Field that indicates the maximum number of minutes that are permitted to pass before reconnection to a TSO session becomes impossible. This setting can be changed from its default of 3 with the RECONLIM parameter in PARMLIB member TSOKEY*xx*.

TSOUSERMAX

This field shows the maximum number of TSO users that can be connected to the system at the same time. This setting can be changed from its default of 40 with the USERMAX parameter in PARMLIB member TSOKEYxx.

TSOUSERS

This field shows the number of TSO users that were actually active on the system during the snapshot.

UNDEFINEDUSER

This string indicates the userid to be used for local jobs that enter the system without a userid; it cannot be set to a userid defined in the RACF database.

The UNDEFINEDUSER can be set by a SETROPTS JES(UNDEFINEDUSER) command; the default is '++++++++'. This field supports overtype.

VMLEVEL, VMLVL

String indicating the software level of VM. This field is empty if zSecure Collect was insufficiently authorized or licensed to collect hypervisor information.

VMSYSTEM

The name of the VM system under which MVS is running. This field is empty if zSecure Collect on z/VM was insufficiently authorized or licensed to collect hypervisor information.

VMUSERID

VM userid of the machine running MVS. It is empty when MVS is not running under VM.

VTAMLEVEL, VTAMLVL

String indicating the software level of VTAM in the format `3.4.1/ESA`.

VTAMNETID, NETID

The network id set by the VTAM start option NETID. This is used in constructed profile names in some classes; for example, the first qualifier of NetView RMTCMD and APPC APPCLU.

WARNING, PWDWARNING

This string indicates the maximum number of days before the expiration of a password, at which RACF is to issue a warning message to a user (due to a `SETROPTS PASSWORD(WARNING)` command). If set to `NO`, no warning is issued. Otherwise, this field contains a number in the range 1-255.

This field is modifiable.

WHENPROGRAM, PROGRAM

This flag indicates whether RACF program control is active (due to a `SETROPTS WHEN(PROGRAM)` command). If the value of `WHENPROGRAM` is *YES*, RACF protection is in effect for access to load modules and Program Access to Data Sets (PADS), independently of whether the PROGRAM class is active or not.

This field is modifiable.

XBMALLRACF

Flag field that indicates ifJES2 is to test jobs to be run with an execution batch monitor for either a valid RACF userid and password or propagated RACF information. If the value of XBMALLRACF is `YES`, all jobs that do not contain the user identification fail.

The option indicated by this flag can be set by a SETROPTS JES(XBMALLRACF) command.

This field is modifiable.

TEMPLATE: RACF Database Templates

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•	•		

This section documents the fields for NEWLIST TYPE=TEMPLATE. Unless otherwise stated, all fields can be used for SELECT/EXCLUDE processing as well as in the output commands LIST, SORTLIST, DISPLAY and SUMMARY. The NEWLIST TYPE=TEMPLATE displays the templates that describe the fields available in the RACF database as well as custom fields. It generates one entry per field type; a unique key is FIELD ENTITY SEGMENT.

The RACF database templates and custom field definitions from the Dynamic Parse Table are used in the NEWLIST TYPE=RACF to define select/exclude and output fields; the templates and custom fields can also be displayed using the SHOW TEMPLATES command. Only custom fields that do not have the same name as a database template field in the same segment are listed.

Field descriptions

The `TEMPLATE NEWLIST` supports the following fields for reporting.

AIM_ALIAS

Flag field that indicates if the field is an Application Identity Mapping alias name.

ALIAS

If the current field is an alias field, this field contains the name of the original field used whenever this alias name is referenced. If the current field is not an alias field, the value is missing.

COMPLEX

This field identifies the security complex name. The value can come from the ALLOC COMPLEX parameter or default to the security node or sysplex name. The default field length is 8 characters.

If the ALLOC statement for a CKFREEZE data set contains a VERSION= parameter, a blank and the 4-character version are appended to the 8-character complex name. To display the version in the report output, use an output length modifier on the COMPLEX field and specify a value of 13 or greater, or 0. See "Modifying output length" on page 797.

COMMAND_PARM

This field indicates which RACF command parameter can be used to change the field.

COMMAND_PARM_FORMAT

Indicates the name of the output format required for generating a command parameter for a RACF command. If the value is missing, no special formatting is needed to use the field as a command parameter. If the format starts with an underscore then there is no output format available that can directly generate the command parameter value. If the value starts with "_No", the command parameter needs to be formatted as "NO" followed by the keyword, or the keyword with the field formatted according to the rest of the parameter format between parentheses. It can have the following values for the format:

- $Auditlvl, $ACL, $CmdAuth, $CondQt, $Connect, $DOM, $Logdays, $Logtime, $Monitor, $MsgLevl, $MForm, $Quoted, $Yes, $No
- _Add/Del, _CharNone, _CKG, _Echo, _No$CondQt, _No$Quoted, _No$Timeout, _NoChar, _NoKeyword, _NoNum, _Other
- Access, Char, Num, or USdate

DATE3

Flag field that indicates if the field represents a 3-byte date.

DEFAULT

This hexadecimal field contains the default value of the field. This value is only set in a restructured database, and will be missing otherwise. The default value of the field is used if the field is not set in the database.

DESCRIPTION

Contains a Security zSecure description of the use of the field.

EBCDIC_ALIAS

Flag field that indicates if a field that is an Application Identity Mapping alias name contains values in EBCDIC. This field is missing for fields that do not have the AIM_ALIAS flag set.

ENTITY

Contains the name of a RACF profile kind, the entity type. This will be USER, GROUP, DATASET, or GENERAL. When combined with the SEGMENT and FIELD fields, it uniquely identifies an entry in the NEWLIST TYPE=TEMPLATE.

FIELD

Contains the name of a RACF profile field. This name can be used in SELECT, EXCLUDE, LIST, SORTLIST, and SUMMARY commands for the RACF profile report (NEWLIST TYPE=RACF). When combined with the SEGMENT and ENTITY fields, it uniquely identifies an entry in the NEWLIST TYPE=TEMPLATE.

FLAG

Flag field that indicates if RACF considers the database field a RACF flag field, SPECIAL or group-OPERATIONS for example.

FORMAT

This field describes the default Security zSecure output format used for the field.

GROUP

If the current field is part of a repeat group, this field contains the name of the count field that indicates the number of entries in the repeat-group. If the current field is not a repeat group, the value is missing. See also the REPEATED field.

HAS_TEMPLATE

This flag indicates whether a field name is represented in the templates. This flag is ON for all fields except the custom fields from the Dynamic Parse table. The Dynamic Parse table is loaded from the class CFIELD profiles CFDEF segments when IRRDP100 is run.

HAS_DPI

The field name is present as a keyword name in the RACF Dynamic Parse table. For custom fields, the Dynamic Parse table gets loaded from the RACF class CFIELD profile CFDEF segments when IRRDPI00 is run. For non-custom fields in non-base segments, RACF has built-in dynamic parse information such as a maximum input length (MAXLEN), for numeric variables a minimum and/or maximum value (MINVAL or MAXVAL), and for character fields whether they support mixed case (MIXED). The HAS_DPI provides an indication where such information has come from. If HAS_DPI is off and the information is present nonetheless, it comes from the built-in zSecure knowledge base. If HAS_DPI is on and HAS_TEMPLATE is off, you can modify them yourself in the CFDEF segment.

HEADER

Contains the default Security zSecure output header of the field.

HIDDEN

Flag field that indicates if the field is considered to be confidential. Confidential fields are not unloaded by IRRDBU00, and zSecure does not write these fields to an UNLOAD file. If an unloaded database is used for input, the contents of the field is not available.

ID

Contains the sequence id of the RACF field within the segment.

FIRST

Indicates the character set for the first character of a field value. This is derived from the RACF Dynamic Parse Table. The output format is CFSYN by default (shown as selection AN#S). It can also be printed with the $CFSYN format to get strings that RACF uses on the CFDEF segment variable CFFIRST, NONATNUM for example.

HELP

Contains the first line of TSO help text for the keyword from the RACF Dynamic Parse table. The default output length is 64, the maximum length in practice is 255.

LENGTH

The default length of the field on output produced by Security zSecure. If the length is given as Varies, there is no default length, and a ragged column layout may result unless you specify an overriding length value.

MASKED

Flag field that indicates if the value of the field is encrypted in the RACF database, values for passwords for example. zSecure does not write masked fields to an unload file. As a result, this field is not available when an unloaded database is used for input.

MAXLEN

Identifies the maximum length that can be input for the field. It can be either built-in on knowledge or be derived from the RACF Dynamic Parse Table. The default width is 6; the default format is NUM.

This value can only be modified for custom fields. To modify the value, change the CFDEF segment and refresh the Dynamic Parse table. MAXLEN cannot be modified directly on the TYPE=TEMPLATE display.

MAXVALUE

Specifies the maximum value for a numeric variable. The default output length of this field is 10; the default format is NUM.

MINLEN

Specifies the minimum value for a numeric variable. The default output length of this field is 10; the default format is NUM.

MIXED

Flag field that indicates if a field allows case-sensitive input. YES indicates that upper and lower case characters are accepted and preserved. NO indicates that all input is converted to uppercase. The value can come from a template or from dynamic parse information. The default format is $YESNO.

This value can only be modified for custom fields. To modify the value, change the CFDEF segment and refresh the Dynamic Parse table. MIXED cannot be modified directly on the TYPE=TEMPLATE display.

OTHER

Identifies the character set for characters beyond the first. The output format is CFSYN by default (shown as selection AN#S). It can also be printed with the $CFSYN format to get strings that RACF uses on the CFDEF segment variable OTHER, NONATNUM for example.

PAD

Flag field that indicates if RACF pads the field with zeroes on the left if short values are retrieved from the RACF database.

REPEATED

If the current field is part of a repeat group, this flag field is set to YES, otherwise it is set to NO. See also the GROUP field.

SEGMENT

Contains the name of the RACF profile segment the field is a part of. When combined with the FIELD and ENTITY fields, it uniquely identifies an entry in the NEWLIST TYPE=TEMPLATE.

SIZE

Numeric field that indicates the size (in bytes) that the field takes in the RACF database. If the field is of variable length, the value is missing.

SORTED

Flag field that indicates if the field is sorted in the RACF database. Typically, this option is used for repeat group fields that are always referred to in sorted order, CGNGRPNM as opposed to the unsorted values CONGRPNM for example.

STAMP

If the RACF database is an unload, this field displays the local date and time of the unload. If the database is live, it displays current date and time. For a copy of a database, it is displayed as '00:00:00.000000'. It cannot be used for SELECT/EXCLUDE processing.

STATISTIC

Flag field that indicates if the field contains a statistic, REVOKECT and LREFDAT for example. Update of statistics is controlled by the SETROPTS INITSTATS and SETROPTS STATISTICS options.

VLF

Flag field that indicates if changes to the field cause RACF to purge ACEEs from VLF.

TRUSTED: Users that can bypass security

The TRUSTED NEWLIST (NEWLIST TYPE=TRUSTED) provides information about which users can bypass the security for z/OS and your security system and why they have these privileges. Each record in this NEWLIST represents a privilege that allows a specific user on a specific complex to ultimately bypass the security for z/OS and your security system software on the indicated complex and system, which can be the same system or another system. The key for a TRUSTED NEWLIST record consists of the fields that define subject privilege and object sensitivity:

- The Sensitive object key is COMPLEX SYSTEM CLASS RESOURCE VOLSER SENSITIVITY.
- The subject privilege key is USERID USERID_PRIVILEGE USERID_COMPLEX VIA.

Only the USERID_COMPLEX for the default system contains the complete resource analysis. The other complexes are mainly privilege based.

Trusted users must not be defined with a default user ID accessible without authentication by password or other method. Only define the minimum number of trusted users required to represent the total user population. A big site might define between ten and 15 trusted users. You can use the TRUSTED NEWLIST to verify that trusted users are legitimately and correctly defined, and use the records to determine which set of trust relations to eliminate if you want to revoke trust privileges for a user.

Field descriptions

The TRUSTED NEWLIST provides the following fields for reporting.

ACCESS

This field contains the access level of the user on the resource, when operating from the "USERID_COMPLEX" on page 1478. The minimum access level that still would make the user trusted is listed in another field, RISK. (See "RISK" on page 1477.)

The ACCESS field is missing for privileges that do not relate to a resource.

Table 557 list the access levels that can be shown for trust relations established through MVS resources on a RACF system.

Table 557. TRUSTED access levels granted through MVS resources

Access	Explanation
ALTER	ALTER access
ALTER-M	Authority to alter some fields in his own user profile
ALTER-O	Authority to alter caused by a group-operations attribute
ALTER-P	Authority to alter a discrete profile (allowing you to issue PERMIT)
CONTROL	CONTROL access
CKGOWNR	Authority to access/change information using CKGRACF through the CKG.SCP scope profiles. The real access depends on CKG.CMD profile access. This can only be more access than standard RACF, not less

Table 557. TRUSTED access levels granted through MVS resources (continued)

Access	Explanation
CREATE	Authority to create a more specific profile, or CREATE authority in a group
EXECUTE	EXECUTE access
NONE	No access
OWNER	Authority through ownership
QUALOWN	Authority based on the qualifier of a data set profile. If the data set HLQ is an userid, this userid has QUALOWN authority. Otherwise, if the data set HLQ is a groupid, any user with group-special
READ	READ access
UPDATE	UPDATE access

Table 558 list the access levels that can be shown for trust relations established through UNIX resources.

Table 558. TRUSTED access levels granted through UNIX resources

Access	Explanation
EXECUTE	`--x` access
NONE	`---` access
READ-NX	`r--` access
READ	`r-x` access
UPD-NX	`rw-` access
UPDATE	`rwx` access
WRIT-NX	`-w-` access
WRITE	`-wx` access

AUDITPRIORITY

Contains the audit priority that measures the risk the privilege poses. The value is 40 or higher if the privilege is a major exposure. For example, the user ID value represents some default user anybody can use.

AUDITCONCERN

Explains how the privilege can be used to obtain the highest system authorization. This field might also contain additional information to explain high audit priorities.

Table 559. TRUSTED: Audit concerns

Audit priority	Audit concern
2	Can modify zFS data set while unmounted, might be mounted SETUID later.
5	Can modify SETUID zFS data set while unmounted, can gain UID(0).

CLASS

Contains the resource class of the resource that the user has access to. For privileges, it identifies the type of object or subject where the privilege or security attribute resides.

COLLECT_DATETIME

Returns the time stamp that indicates when the CKFREEZE file was created. If no CKFREEZE file is in use on a live system, the date and time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

Contains the name of the security complex the SYSTEM belongs to, and hence the sensitive resource. The combination of the COMPLEX SYSTEM fields identifies the system that the user can manipulate. This can be specified by the COMPLEX= keyword on an explicit ALLOC statement, or it defaults to a system name.

RACF_CLASS

The class name of the RACF_PROFILE. RACF_CLASS can refer to the associated grouping class, while CLASS refers to a member profile class. The RACF_CLASS protects the RACF profile key when it is accessed from the security complex of USERID_COMPLEX. See "USERID_COMPLEX" on page 1478.

RACF_PROFILE

The RACF profile key in the class RACF_CLASS that protects the profile key when it is accessed from the security complex of USERID_COMPLEX. See "USERID_COMPLEX" on page 1478.

RESOURCE

Contains the resource name in the domain of the SAF resource class listed in CLASS. The maximum length of the field is 255 bytes. This field is missing for privileges that are not associated with a specific resource.

RESOURCE_LOCATION

Identifies the resource name environment. This field is repeat group field. The default and maximum length is 35 characters. An example value is IPO1.CICS.CICSTS41.DATASET. The format is as follows:

system.subsy-type.subsys-identification.restype

RISK

Contains the minimum access level that still makes the user trusted. The actual access granted to the user is found in the ACCESS field. (See "ACCESS" on page 1475.)

The RISK field is missing for user privileges.

SENSITIVITY

Contains the type of sensitivity the resource has on the system identified by the COMPLEX SYSTEM fields. In addition the following sensitivity types can be listed:

Table 560. TRUSTED: Additional sensitivity types

Sensitivity	Meaning
CICS Loadlb	CICS program library
CICS CSD	CICS resource definition data set
CICS Parms	CICS parameter library
CICS ACF2pr	ACF2/CICS parameter library
DB2 BootSDS	DB2 Bootstrap data set (BSDS)

Table 560. TRUSTED: Additional sensitivity types (continued)

Sensitivity	Meaning
Dflt ID map	This user is mapped to by the default distributed identity filter (* for both registry and filter).
ID mapping	This user is mapped to by a distributed identity filter.
IMS PROCLIB	IMS program library
Privilege	The user has a special privilege or security attribute (not through SAF on all ESMs). For RACF these include OPERATIONS, SPECIAL. For HSM these include HSM CNTL, HSM USER.
Resource	The user has SAF access on a sensitive general resource (classes include DASDVOL, FACILITY, FIELD, HFSSEC, LOGSTRM, PRIVCTL, TSOAUTH, UNIXPRIV, VMMDISK, VMSEGMT).
zFS	zFS data set

In case of multiple sensitivities for a single data set, only the prime sensitivity or sensitivities are represented. For instance, a data set can be a MSTR parmlib, a JES2 parmlib, an STC proclib and a JOB proclib all at the same time. In this case it will be shown as a JES2 parmlib, because that data set may contain human readable passwords.

SYSTEM

Contains the name of the target system where the sensitive resource resides. That is, the system that can be manipulated or attacked by the user.

USERID

Contains the user ID value that has access to the privilege described in the record.

USERID_COMPLEX

Contains the name of the security complex where the `USERID` is defined. That is, the complex from which the user can access the resource. This value can be specified by the `COMPLEX=` keyword on an explicit `ALLOC` statement, or it defaults to a system name.

USERID_PRIVILEGE

Contains the name of the user privilege, security attribute, or sensitive operating system function the user has access to. This value is a privilege on the complex where the user is defined, `USERID_COMPLEX`. The maximum length of the field is 9 bytes. The field can contain any of the following values

- *CLASS*: *A*, *B*, *C*, *D*, *E*, *F*
- *AUTH*:*ClassAuth*, *ConnAuth*, and *DUMPAUTH*
- *GROUP*: *GroupOper*, *GroupSpec*
- *HSM*: *HSM USER*, and *HSM CNTL*
- *JOBFROM*
- *MAINT*
- Mapped ID
- *MUSASS*
- *NON-CNCL*
- *Operations*

- *Owner*
- *Permit*: *PermitGrp*, *PermitUsr*, *Permit Prefix*
- *READALL*
- *Rule*: *Rsrc rule*, *No Protect*, *NoRule*, and *Rule*
- SECURITY
- *Special*
- *Superuser*
- *TAPE-BLP*
- *UACC*
- *Unix*: *UnixGroup*, *UnixOther*, *UnixOwner*,, and *UnixUser*
- *Warning*

VIA

Contains the group or userid that provided access. The group is returned if access is given through a group. Group access is indicated when the USERID_PRIVILEGE field contains any of the following values: *PermitGrp*, *GroupSpec*, *GroupOper*, or *UnixGroup* in field. If access was given through class authorization, this field contains the userid.

VOLSER, VOLUME

Contains a volume serial further identifying the resource name in field RESOURCE. This field is missing for privileges not relating to a resource, and for resources that are not associated with a specific volume serial.

TYPE: Newlist type definitions

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The TYPE NEWLIST (NEWLIST TYPE=TYPE) lists the NEWLIST types supported by the product and provides the original English and default translated properties for each type.

The key for records in TYPE NEWLIST is NEWLIST_TYPE. An alternate key is NEWLIST_TAG.

Field descriptions

Table 561 list the fields available in the TYPE NEWLIST. Descriptions for each field follow the table.

Table 561. NEWLIST TYPE=type parameter descriptions

Field	Column Header	Length
ABBREV2	T2	2
DETAILHELPPANEL	Det help pnl	8
HELPPANEL	Help pnl	8
NEWLIST_TAG	Tag	3
NEWLIST_TYPE	Type	24
TOPTITLE	Toptitle	64

Table 561. NEWLIST TYPE=type parameter descriptions (continued)

Field	Column Header	Length
TOPTITLE_ORIG	Original toptitle	64

ABBREV2
A unique two character representation of the NEWLIST type. It is used in some default panel names and can be used in generation of ddnames. This number can change without warning and is not a programming interface.

DETAILHELPPANEL
The default help panel name used for a detail display of this type.

HELPPANEL
The default help panel name used for a summary or overview level display of this type.

NEWLIST_TAG
An internal number for the NEWLIST type. This number can change without warning and is not a programming interface.

NEWLIST_TYPE
The NEWLIST type in character format.

TOPTITLE
The default top title used for translated output of this NEWLIST type.

TOPTITLE_ORIG
The original English default top title for output of this NEWLIST type.

UNIX: UNIX System Services File System

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•			•	•	•	•

The UNIX NEWLIST (NEWLIST TYPE=UNIX) describes the unified file system used by the z/OS UNIX System Services on each system. To use this type, you must have one or more CKFREEZE files that provide information about the data set content of the file system and the current mount points. For a summary of the mount points, see "MOUNT: UNIX Mount Points" on page 1104. This NEWLIST type only provides information about the UNIX files system data sets that are mounted.

- Each record in this NEWLIST represents an (effective) directory entry.
- A record is uniquely identified by the fields SYSTEM, COMPLEX, DEV and REL_PATHNAME
  - SYSTEM and COMPLEX define the system being considered. These fields are also an alternate key.
  - The DEV number represents a mount point with the following characteristics FS_SYSTEM, FS_COMPLEX, FS_DSN, FS_VOLSER, FS_SERIAL that determine the relation between REL_PATHNAME and ABS_PATHNAME and thus the file system mounted there.
  - REL_PATHNAME indicates the directory entry within the file system.
- The fields SYSTEM, COMPLEX and ABS_PATHNAME are an alternate key.
- Within a file system, several directory entries can describe the same file (multiple REL_PATHNAMEs, one INODE). In UNIX there is no such thing as the *real name* of a file. The effective attributes take the settings along the separate paths to the file into account.

Field descriptions

The UNIX NEWLIST provides the following fields for reporting.

ABS_PATHNAME

The absolute path name for this record.

ATTR

The file's attributes (including access modes), by default printed as 'rwxrw-r--'. In this example, the owner has read, write and execute access, the file's group read and write access, others have only read access. The setuid, setgid and sticky bits are also taken into account in the consecutive 'x' positions, resulting into 's' or 't' (when the execute bit itself is off: 'S' or 'T'). See “Formatting UNIX file type, attribute, and audit flag fields” on page 823 for alternate formats OCTAL and $CHMOD, and extended syntax selection. See also “TYPE” on page 1489 and “EXTATTR” on page 1486.

The ATTR field shows the effective attributes, which are a combination of the physical attributes set for the file itself with the mount attributes of the file system it is in and the effective attributes of the directories in the path to the file. If the file system is mounted NOSETUID or NOSECURITY the setuid and setgid attributes are disabled. NOSECURITY disables the sticky bit for directories as well, and access is allowed without the read, write or execute attributes as well. If the file system is mounted READ-only (instead of RDWR), write access is effectively disabled. The attributes physically stored in the file system data set can be found in “PHYSICAL_ATTR” on page 1489 See also “unxhfse” on page 1487 and “FS_SERIAL, HFS_SERIAL” on page 1487.

AUDITCONCERN, CONCERN

Indicates the reason for the audit priority. You should not make use of the exact value of this field. The value can contain one or more audit concerns separated by commas. The following audit concerns have currently been defined:

Table 562. Audit concern descriptions

Audit concern	Description
executable file bypasses file security (setuid 0)	This executable file runs with superuser authority even when executed by a normal user. There are normal utilities that need this authority. These files should be monitored closely, their origin should be known and changes in contents and attributes should be audited.
executable file masquerades as another user and group (setuid/setgid)	This executable file does not run with the current user's uid and gid, but with another uid and gid.
executable file masquerades as another user (setuid)	This executable file does not run with the current user's uid, but with another uid.
executable file masquerades as belonging to a different group (setgid)	This executable file does not run with the current user's gid, but with another gid.
executable file runs program-controlled (extattr +p)	This executable file must run in a clean, controlled environment. If it does, it may have additional authorities (like daemon, server).

Table 562. Audit concern descriptions (continued)

Audit concern	Description
executable file runs APF-authorized (extattr +a)	This executable file runs as if loaded from an APF-authorized library. For example, if this program is exec()ed at the job step level and the program is linked with the AC=1 attribute, the program will be executed as APF-authorized.
special file is world writable	This special file (/etc/rc, /etc/profile, or /etc/automount.master) can be overwritten by anyone with access to z/OS UNIX System Services. Files reported with this concern need to be investigated especially, because they are important configuration files. For symbolic links (including external links) this condition is not reported, because the attribute setting is standard and typically ignored (the authorizations of the link's target are checked instead).
file is world writable	This file can be overwritten by anyone with access to z/OS UNIX System Services. This concern needs to be investigated especially for configuration files like files in the /etc directory. For symbolic links (including external links) this condition is not reported, because the attribute setting is standard and typically ignored (the authorizations of the link's target are checked instead).
special directory is world writeable but existing entries are protected (sticky bit)	When the Sticky bit is set on a directory, only the owner of a file in that directory (or a superuser) is allowed to delete or rename that file. However, anyone with access to z/OS UNIX System Services is allowed to create a new file in this special directory (the root directory or /etc). For some files their existence is enough to alter security decisions, e.g. ftp or cron allow or deny files. Other files are executed automatically if they exist, e.g. a file .profile in the home of a user, and this file will be run under this user's privileges. Note that root is the default for a user's home directory.
directory is world writeable but existing entries are protected (sticky bit)	When the Sticky bit is set on a directory, only the owner of a file in that directory (or a superuser) is allowed to delete or rename that file. However, anyone with access to z/OS UNIX System Services is allowed to create a new file in this directory.
home directory is world writeable but existing entries are protected (sticky bit)	When the Sticky bit is set on a directory, only the owner of a file in that directory (or a superuser) is allowed to delete or rename that file. However, anyone with access to z/OS UNIX System Services is allowed to create a new file in this directory. In addition, it the home directory of the user specified by the HOME_OF field.

Table 562. Audit concern descriptions (continued)

Audit concern	Description
special directory is world writable	This special directory (the root directory or /etc) allows anyone with access to z/OS UNIX System Services to change entries in it. This needs to be investigated especially because they contain configuration files. Write access on the directory allows anyone to rename a file. This could make it possible to switch configuration files. As an example it would be possible to swap a current /etc/ftp.data (maybe with tighter security) with another copy that was saved by an administrator. The copy might enable anonymous ftp, while this is not allowed by the current version of /etc/ftp.data. If the directory is also world readable it would ease finding a suitable "other" configuration file.
directory is world writable	This directory allows anyone with access to z/OS UNIX System Services to change entries in this directory. This concern needs to be investigated especially for directories that contain configuration files. Write access on the directory allows anyone to rename a file.
home directory is world writable	This directory allows anyone with access to z/OS UNIX System Services to change entries in this directory. In addition, it the home directory of the user specified by the HOME_OF field.
/tmp is world writable and existing entries are not protected (no sticky bit)	The /tmp directory allows anyone with access to z/OS UNIX System Services to change entries in this directory. Write access on the directory allows anyone to rename a file. It is recommended that this directory has the sticky bit set.
.profile in user's home directory is world writable	This file can be overwritten by anyone with access to z/OS UNIX System Services. In addition, this is a special file that is automatically executed when a user to whom it applies logs on to z/OS UNIX System Services, thereby forming a major risk where Trojan horse attacks are concerned. Check the HOME_OF field for the directory where the file resides to see which user it applies.
Emacs initialization file in user's home directory is world writable	This file can be overwritten by anyone with access to z/OS UNIX System Services. In addition, this is a special file that is automatically executed when a user to whom it applies starts the Emacs editor, thereby forming a major risk where Trojan horse attacks are concerned. Check the HOME_OF field for the directory where the file resides to see which user it applies.

Table 562. Audit concern descriptions (continued)

Audit concern	Description
`sh_history in user's home directory is world writable`	This file can be overwritten by anyone with access to z/OS UNIX System Services. In addition, this is a special file containing a history of previously entered shell commands to be used for retrieval and re-execution; commands in it may therefore easily be executed by a user to whom it applies; thereby forming a risk where Trojan horse attacks are concerned. Check the HOME_OF field for the directory where the file resides to see which user it applies.
`Seclabel does not conform to the recommendation of` *`seclabel`*	A specific security label is recommended for this file or directory, as documented in the book "Planning for Multilevel Security and the Common Criteria", chapter "Establishing Multilevel Security".
`cron not disabled. Security labels can be bypassed`	cron is a clock daemon that runs commands at specified dates and times. It does not check security labels, and should be disabled for general use in a multilevel-secure environment. This can be done by giving it SYSHIGH, or a unique security label that is not dominated by a general user security label.
`Automount managed directory does not conform to the recommendation of SYSMULTI`	All automount managed directories should have the SYSMULTI security label assigned to ensure the availability of mounted data, regardless of security label.
`Security label substitution is not performed`	Security label substitution for a symlink with a linktarget of $SYSSECA or $SYSSECR will only be done when the SECLABEL class is active, and the system runs z/OS 1.5 or later.

Any of the preceding audit concerns can be suffixed with `but path-protected`. This indicates that the file security information as kept with the inode allows what the audit concern states, but the path to the inode described in this record does not. There might be different paths (hardlinks) to the same inode that do not prevent the audit concern condition from being exploited.

AUDITFLAGS

This 3-character field contains the effective audit flags for read, write and execute attempts (in that order). Each can be 's' (success audit), 'f' (failure audit), 'a' (all access) or '-' (no auditing). Auditing occurs effectively when either the auditor or the user has requested it. See “AUDITFLAGS_AUDITOR” and “AUDITFLAGS_USER” on page 1485. See “Formatting UNIX file type, attribute, and audit flag fields” on page 823 for alternate format $CHAUDIT and the extended syntax supported for SELECT/EXCLUDE processing.

AUDITFLAGS_AUDITOR

This 3-character field contains the auditor-specified audit flags for read, write and execute attempts (in that order). Each can be 's' (success audit), 'f' (failure audit), 'a' (all access) or '-' (no auditing). See 1484 and “AUDITFLAGS_USER” on page 1485. See “Formatting UNIX file type, attribute, and audit flag fields” on page 823

on page 823 for alternate format $CHAUDIT and the extended syntax supported for SELECT/EXCLUDE processing.

AUDITFLAGS_USER

This 3-character field contains the user-requested audit flags for read, write and execute attempts (in that order). Each can be 's' (success audit), 'f' (failure audit), 'a' (all access) or '-' (no auditing). See 1484 and "AUDITFLAGS_AUDITOR" on page 1484. See "Formatting UNIX file type, attribute, and audit flag fields" on page 823 for alternate format $CHAUDIT and the extended syntax supported for SELECT/EXCLUDE processing.

AUDITID

The file's audit id. It is currently only available for files in an HFS. When selecting on this field, you should use the exact hexadecimal value.

```
select auditid='01E2D4F3F0F0F933EA1C000002300000'x
```

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 563. UNIX NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

This field contains the name of the (viewpoint) security complex. This can by specified via the COMPLEX= keyword on an explicit ALLOC statement, or it may default to a system name.

DEPTH

This field contains the directory level for the file.

DEV

This field contains the device number, which is an identification of the file system data set in which the file described by this record resides, via the list of mounted file systems for this system. DEV and INODE uniquely identify a physical file within a unified file system; if LINK_COUNT is greater than one, it has multiple directory entries ('hard links'). See also INODE and FS_DSN.

DIRECTORY_DEFAULT_ACL

This flag field is only present for a directory. It indicates if the directory has a directory default access list or not. See “UNIX_DEFAULT_ACL” on page 1492 for the content of the access list.

DIRNAME

The pathname without the last qualifier, for example, the name of the directory this entry is in. Note that a mount point is represented both as a directory in its parent file system and as '.' within the file system mounted there. For the latter entry DIRNAME will equal ABS_PATHNAME.

EXTATTR

The extended attributes, e.g. 'a---' for APF-authorized, '-p--' for program controlled, '--s-' to indicate _BPX_SHAREAS (OMVS share address space setting) is honored, '---l' to indicate library sharing is allowed. Note that 's' is set by default, if a file does not have the attribute it will always be started in its own address space. See “Formatting UNIX file type, attribute, and audit flag fields” on page 823 for the alternate format $EXTATTR and the extended syntax supported for SELECT/EXCLUDE processing.

The EXTATTR fields shows the effective attributes, which are a combination of the physical extended attributes set for the file itself with the mount attributes of the file system it is in. If the file system is mounted NOSETUID or NOSECURITY the APF and program control attributes are disabled. The extended attributes physically stored in the file system data set can be found in “PHYSICAL_ATTR” on page 1489. See also “unxhfse” on page 1487 and “FS_SERIAL, HFS_SERIAL” on page 1487.

EXTENDED_ACL

Flag field that indicates whether the file or directory has an extended access ACL (access list). See “UNIX_ACL” on page 1489 for the actual access list content.

EXTERNAL_LINK

Flag field that indicates whether the entry is a link to an MVS data set or member. The target of the link can be found in “LINK_TARGET” on page 1488.

FILE_DEFAULT_ACL

Flag field indicates if the directory has a file default access list or not. This value is only present for a directory. See “UNIX_FDEFAULT_ACL” on page 1492 for the content of the access list.

FILENAME

The last qualifier of REL_PATHNAME. Note that a mount point is represented both as a directory in its parent file system and as '.' within the file system mounted there. The latter entry shows the FILENAME as '.'.

FS_COMPLEX, HFS_COMPLEX

Contains the name of the security complex of which the system that owns the file system data set indicated by DEV is a part. See also “FS_SYSTEM, HFS_SYSTEM” on page 1487.

FS_DSN, HFS_DSN

The MVS data set name of the file system associated with DEV. Note it may not be directly accessible from SYSTEM. See “FS_SYSTEM, HFS_SYSTEM” on page 1487.

FS_MOUNTPOINT, HFS_MOUNTPOINT

Absolute pathname for the mount point of the file system associated with DEV.

FS_RDWR, HFS_RDWR

Flag field that indicates if the file system associated with DEV is mounted in read/write mode.

FS_SECURITY, HFS_SECURITY

Flag field that indicates if the file system associated with DEV is mounted with the SECURITY option, for example, whether security checks are performed. Note that if this is not the case, setuid, setgid, APF, and program control bits are ignored, and for directories the sticky bit as well.

FS_SERIAL, HFS_SERIAL

Describes the DASD unit's volume serial number and device id for the file system's data set. This field may not be filled in if the CKFREEZEs allocated do not contain a detailed description of the FS_SYSTEM as well as SYSTEM (as they may differ). This field can be used to disambiguate between DASD volumes with the same FS_VOLSER. See also "BOX_SERIAL field for DASDVOL report" on page 1014 for further details.

FS_SETUID, HFS_SETUID

Flag field that indicates if the file system associated with DEV is mounted with the SETUID option, for example, whether setuid, setgid, APF, and program control bits are to be honored. The file system must also be mounted with the SECURITY option for these bits to be honored.

FS_SYSTEM, HFS_SYSTEM

Contains the name of the system that owns the file system data set indicated by DEV. (It is possible to share a unified file system within a sysplex; the actual file system data set can be managed by one system, while all systems have access to it, even if they do not share the DASD.)

FS_VOLSER, FS_VOLUME, HFS_VOLSER

The (first) volume serial of the file system associated with DEV. This field may not be filled in if the CKFREEZEs allocated do not contain a detailed description of the FS_SYSTEM as well as SYSTEM (as they may differ).

GID

The group for the file (GID). See also "GROUP."

GROUP

The group for the file , shown as a RACF identity if one is available (reverse translation). If several reverse translations are possible, the alphabetically first is shown. See also "GID," "OWNER" on page 1488 and "UID" on page 1489.

HFS_COMPLEX

This field is an alias for the FS_COMPLEX field. See "FS_COMPLEX, HFS_COMPLEX" on page 1486 for details.

HFS_DSN

This field is an alias for the FS_DSN field. See 1486 for details.

HFS_MOUNTPOINT

This field is an alias for the FS_MOUNTPOINT field. See "FS_MOUNTPOINT, HFS_MOUNTPOINT" on page 1486 for details.

HFS_RDWR

This field is an alias for the FS_RDWR field. See “FS_RDWR, HFS_RDWR” on page 1487 for details.

HFS_SECURITY

This field is an alias for the FS_SECURITY field. See “unxhfse” on page 1487 for details.

HFS_SERIAL

This field is an alias for the FS_SERIAL field. See “FS_SERIAL, HFS_SERIAL” on page 1487 for details.

HFS_SETUID

This field is an alias for the FS_SETUID field. See “FS_SETUID, HFS_SETUID” on page 1487 for details.

HFS_SYSTEM

This field is an alias for the FS_SYSTEM field. See “FS_SYSTEM, HFS_SYSTEM” on page 1487 for details.

HFS_VOLSER

This field is an alias for the FS_VOLSER field. See “FS_VOLSER, FS_VOLUME, HFS_VOLSER” on page 1487 for details.

HOME_OF

This repeated field can only be filled in for a directory. It lists the RACF users for whom this directory is their home directory.

INODE

Contains an inode number, which uniquely identifies a physical file within a physical file system. Together with DEV this identifies a single file in a unified file system. A UNIX file generally does not have a unique filename; instead, there may be multiple path names (known as 'hard links') that point to the same INODE. LINK_COUNT contains the number of hard links to the file. For each pathname a separate record with the same DEV and INODE will be produced (for each unified file system view, for example, per system/complex). Permissions and attributes are associated with the INODE, so they are the same for all hard links to it.

LINK_COUNT

The number of hard links to the file described by the current entry. A UNIX file generally does not have a unique filename; instead, there may be multiple path names (known as 'hard links') that point to the same INODE. (If LINK_COUNT is equal to one, there is only one hard link, so that pathname could be considered to be the name of the file.) Symbolic links are not included in this count.

LINK_TARGET

For a symbolic link, this field contains the pathname linked to. A symbolic link is a file which redirects one pathname to another (by name). It does not specify an inode, and it can point to another physical file system. If the file is deleted, the symlink is kept and may again become active when a file of the indicated name is created again.

For an external link, this field contains the MVS data set or member linked to. In the case of a member name, the current MVS search order for the module at execute time applies.

OWNER

The owner of the file, shown as a RACF identity if one is available (reverse translation); if several reverse translations are possible, the alphabetically first is shown. See also "UID," "GROUP" on page 1487 and "GID" on page 1487.

PHYSICAL_ATTR

The attributes for the file as physically stored in the file system data set; the effective attributes can be found in ATTR. See "ATTR" on page 1481.

PHYSICAL_EXTATTR

The extended attributes for the file as physically stored in the file system data set; the effective attributes can be found in EXTATTR. See "EXTATTR" on page 1486.

REL_PATHNAME

The pathname for the record within the file system's data set it is contained in, for example, relative to the mount point associated with this DEV. If you unmount a file system from one mount point and remount it elsewhere, the absolute pathname will have changed but this field will have remained constant.

SECLABEL

The security label of the file. If an assumed security label is in effect, this field contains the READONLY_SECLABEL. See "READONLY_SECLABEL" on page 1106.

SYMBOLIC_LINK, SYMLINK

Flag field that indicates whether the entry is a symbolic link. The target of the link is contained in LINK_TARGET.

SYSPLEX

The name of the sysplex the SYSTEM is a part of (if applicable).

SYSTEM

The name of the (viewpoint) system. For MVS systems, this is the SMF system id; the field length is 8 characters by default for compatibility with other NEWLISTs.

TYPE

The file type. The type is represented by one of the following values: - (regular file), *d* (directory), *ll* (symbolic link), *e* (external link),*p* (pipe/ FIFO),*s* (socket), *c* (character special file), or *b* (block special file). See also "ATTR" on page 1481.

UID

The file owner (a UID). See also "OWNER" on page 1488.

UNIX_ACL

Repeated field that can be used to display the access granted on a UNIX directory entry.

Note: See "EXTENDED_ACL" on page 1486to test for the existence of actual ACL entries.

This field is also completed in correspondence with the ATTR or PHYSICAL_ATTR settings.

The access list content for each directory entry includes the following fields: **User**, access description (**TOrwx**), **ACL id** and **UID/GID**. See "UNIX directory entry access list content - field descriptions." The content included in each entry depends on the access list format setting: `NORMAL`, `EXPLODED`, `RESOLVED` or `EFFECTIVE`. For descriptions of the formats, see "Access list format settings for UNIX" on page 1492.

UNIX directory entry access list content - field descriptions

The contents of the `UNIX_ACL`, `DEFAULT_ACL`, or `UNIX_FDEFAULT_ACL` fields is displayed in tabular format with the following column headings.

`User`

The **User** column shows the RACF user that is allowed access. If a group is not expanded to its containing users, this column shows -**group**- instead. If a UID or GID occurs in the access list, but has no related RACF identity, -**undef**- might be shown in this column. For the global access setting (the 'other' bits on the ACL), this column will show - **any** -.

`Access description (TOrwx)`

The access description field (**TOrwx**) contains the type of ACL in the **T** column, the origin of the entry in the **O** column, and the read, write and execute bits in the **rwx** columns.

- Table 564 lists the possible ACL types (**T**):

Table 564. Access description field - ACL Types

Value	ACL Type
blank	UNIX_ACL
d	UNIX_DEFAULT_ACL
a or **f**	UNIX_FDEFAULT_ACL

- The **O** column displays the origin attribute for the entry. Table 565 shows the possible values.

Table 565. Origin attribute types

Attribute	Description
u	the file owner
g	the owning group
o	other users
+	ACL entries
a	RACF auditor access

The origin is important because of the precedence rules for access determination. The file owner is checked first, followed by user ACL entries. If none of the values match the uid of the requestor, then the owning group and group ACL entries are checked. The group entries are considered equal in rank, and if any entry grants the requested access, it is granted. If file owner, user, or group values do not match, the *other* value is checked. In this case, some additional rules apply: If a user has the RACF RESTRICTED attribute and a protected value for the resource name RESTRICTED.FILESYS.ACCESS in the UNIXPRIV class (UNIXPRIV must be active and RACLISTed), then the *other* bits are not used unless the restricted user has at least READ access.

Users with the RACF AUDITOR attribute have read and execute access to all directories (that is, they can view the file system). Superusers (root users) generally have access too, but this access is not reflected in these fields.

Note: ACL entries are only checked if class FSSEC is active.

- The value of **rwx** (read, write and execute bits) can show either **r**, **w** and **x** for read, write and execute allowed, respectively, or **-** if the corresponding access is not allowed.

ACL id

The **ACL id** column shows the RACF identity for the uid or gid that is actually on the access list. If the uid or gid is shared, entries for all related RACF entries might be present. Alternatively, the **ACL id** column shows `-other-` for the other bits entry. If the uid or gid has no RACF identity, the **ACL id** value (see Table 566) indicates whether the access is for a uid or for a gid.

Table 566. ACL id values for uids or gids without a RACF identity

Value	Meaning
`-owner-`	Access is granted based on the owning uid.
`-group-`	Access is granted based on the owning gid.
`-ACLuid-`	Access is granted based on a uid on the ACL.
`-ACLgid-`	Access is granted based on a gid on the ACL.
`-audit-`	A RACF user is granted read and execute access to a directory because of the system-wide AUDITOR attribute rather than an ACL entry.
`-more-`	If the access list format setting is ACL RESOLVE or ACL EFFECTIVE, **`-more-`** value indicates that access is granted based on a composite of other entries, and therefore not related to a single ACL entry.

UID/GID

The **UID/GID** column shows the uid or gid that grants the access, or an indication why none applies.

Table 567. UID/GID values

Value	Description
n	A number (*n*) indicates the uid or gid depending on the value in the User and ACL id columns. The number indicates a uid if the **User** and **ACL id** columns show the same RACF user, or if the **ACL id** column shows `-owner-` or `-ACLuid-`. The number indicates a gid if the **ACL id** column shows `--group-`, `-ACLgid-`, or a RACF identity (user) different from the one (group) in the **ACL id** column.
n/a	This value indicates that no uid or gid applies because the entry is the global access setting (**ACL id** = `-other-`), a composite entry (**ACL id** = `-more-`, or a RACF user allowed access because of the AUDITOR attribute (**ACL id** = `-audit`).
no uid **no gid**	If the format setting is ACL EXPLODE, the UID/GID be shown that a RACF user would have had access as an AUDITOR but does not have it, because there is no uid or gid associated with the user (either direct, or through BPX.DEFAULT.USER); in that case this column may contain **no uid** or **no gid**.

UNIX_DEFAULT_ACL

Repeated field for displaying the default access granted to directories created within this directory. For details on the access list content included and access list format settings, see “UNIX_ACL” on page 1489. See “DIRECTORY_DEFAULT_ACL” on page 1485 to test for existence of the directory default ACL.

UNIX_FDEFAULT_ACL

Repeated field that can be used to display the default access granted to files created within this directory. For details on the access list content included and access list format settings, see “UNIX_ACL” on page 1489. See “FILE_DEFAULT_ACL” on page 1486 to test for the existence of the file default access list.

Access list format settings for UNIX

The access information shown for each UNIX directory entry depends on the access list format setting. For interactive displays, you can control the format using the ACL command. See “Access list display modes - reference material” on page 30. For generated output, you can specify the format using an output modifier. See the examples in “Formatting UNIX file type, attribute, and audit flag fields” on page 823. The following format settings are available:

ACL NORMAL

For entries with access type UNIX_ACL. the entry includes the following information, depending on the origin:

- If the origin is an owning uid, the uid is used to create an entry for each matching RACF user. If no RACF identity is available, an entry is created with **User -undef-** and **ACL id -owner-**.
- If the origin is an owning gid, the gid is used to create a **-group-** entry for each matching RACF group. If no RACF identity is available, an entry is created with **ACL id -group-**.
- If the origin is other, an entry is added with **ACL id - other -**.

Entries for the access ACL of directories and the file directory default ACL include the following information:

- The uids on the appropriate ACL are processed and used to create an entry for each matching RACF user. If no RACF identity is available, an entry is created with **User** = **-undef-** and **ACL id** = **-owner-**.
- The gids on the appropriate ACL are processed and used to create a **-group-** entry for each matching RACF group. If no RACF identity is available, an entry is created with **ACL id -ACL gid-**. The access bits used are taken from PHYSICAL_ATTR.

ACL EXPLODE

This format setting functions much like ACL NORMAL with the following differences:

- Instead of adding a group entry, entries are added for all users connected to the group.
- If the group is empty, the group entry is retained.
- For the access ACL of directories and the directory default ACL, entries for read/execute access due to the RACF AUDITOR attribute are added as well.

ACL RESOLVE

This format setting functions much like ACL EXPLODE with the following differences:

- Empty groups and -undef- entries are omitted.
- Multiple entries for the same user are resolved. That is, the file owner takes precedence over an ACL entry for the same user.
- Any true user entry takes precedence over one that would be added for a group, and for multiple group entries the highest access is retained if the access levels can be compared, otherwise a composite entry is created.
- RACF AUDITOR access is **not** shown.
- Entries for users without access to UNIX because they have no uid or gid are eliminated.

ACL EFFECTIVE

This format setting functions like the ACL RESOLVE setting with the following differences:

- Instead of using the PHYSICAL_ATTR bits, the ATTR are used. These bits take into account the mount attributes for file system that are mounted. For example, for file systems mounted as read-only, all write access is negated and a check is run for access on higher level directories.
- RACF AUDITOR access is shown, but -no uid- and -no gid- entries are eliminated.

Here are some general guidelines for selecting a format setting:

- Use the EXPLODE format setting to see all members of all groups in the access list (empty groups are kept).
- Use the RESOLVE format setting to see the resolved access for each user.
- Use EFFECTIVE format setting to see the effective access for each user.

VSM: Virtual Storage

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The VSM NEWLIST (NEWLIST TYPE=VSM) describes the Virtual Storage Map. That is, the memory regions that together form virtual storage. This NEWLIST type works both on a *live* z/OS system and a CKFREEZE file produced on such a system.

The VSM NEWLIST describes all storage areas. The CSM NEWLIST describes only the common storage areas. It does not include detailed information on individual common storage areas like the storage area key and subpool values. See "CSM: Common Storage" on page 1009.

Each entry in this NEWLIST represents a storage area region or the slack between two regions, and can be uniquely identified by the fields SYSTEM START.

Field descriptions

The VSM NEWLIST provides the following fields for reporting.

AUDITCONCERN

This field indicates the reason for the audit priority. You should not make use of the exact value of this field. The following audit concern can be returned:
Virtual Storage Audit Concerns: (E)CSA overflow into SQA

AUDITPRIORITY

This numeric field indicates the relative priority of audit concerns. Higher values indicate a higher relative audit priority. For all NEWLIST types, audit priority values map to the following meanings:

Table 568. VSM NEWLIST: Audit priority values and descriptions

Priority	Meaning
40 and greater	Immediate attention required; system security can be circumvented easily.
20 to 39	Review is required; serious security threats might exist.
10 to 19	Review is recommended when time permits.
1 to 9	Informational warnings.
0	No audit concerns identified.

COLLECT_DATETIME

This field contains the time stamp that indicates when the CKFREEZE file for this record was created. When running CARLa commands, if a CKFREEZE file is not provided for the system, the time returned is the current system date and time. This field uses the default output format DATETIME.

COMPLEX

The security complex that contains the system. The complex name can come from the ALLOC COMPLEX parameter or default to a system name.

END

The end address of a storage area. This is either an 8-long (4-byte) hexadecimal number or two 8-long hexadecimal numbers separated by an underscore for 8 byte addresses (possibly) situated above the 4 GB threshold.

FILLED

For the CSA and ECSA storage areas, this field contains the percentage used. If 100% is used, there is most likely an overflow into SQA or ESQA; this is noted by the AUDITCONCERN field.

LENGTH

The length of the storage area. This is a decimal number of up to 20 digits.

START

The start address of a storage area. This value is either an 8-long (4-byte) hexadecimal number or two 8-long hexadecimal numbers separated by an underscore for 8 byte addresses, possibly situated above the 4 GB bar. This field also shows whether the address has a high-order fullword in the operating system or not.

This option does not support sorting information by address. If this function is required, use the `START64` option.

START64

The start address of a storage area in a 64 bit number. This is formatted as two 8-long hexadecimal numbers separated by an underscore for 8 byte addresses (possibly) situated above the 4 GB bar. Use this field to sort by address.

SYSTEM

The name of the system. For MVS systems, this is equal to the SMF system id. The field length is 8 characters for compatibility with other NEWLIST types.

TYPE

A string indicating the virtual storage area type. Table 569 lists the possible TYPE values and their meaning. Areas starting with an *E* reside above 16 MB in virtual storage and areas starting with an *X* reside above 4 GB virtual storage. The name can be followed by `slack` to indicate a slack area, or gap between two storage areas.

Table 569. VSM: Virtual Storage: Storage area types and descriptions

TYPE value	Meaning
CSA	Common Storage Area
ECSA	Extended Common Storage Area
EFLPA	Extended Fixed Link Pack Area
EMLPA	Extended Modified Link Pack Area
ENUC RO	Read-only Extended Nucleus Area
ENUC RW	Writable Extended Nucleus Area
EPLPA	Extended Pageable Link Pack Area
EPVT	Extended Private Area
ESQA	Extended System Queue Area
FLPA	Fixed Link Pack Area
JAVA	JAVA Heap Storage Area
MLPA	Modified Link Pack Area
NUC RO	Read-only Nucleus Area
NUC RW	Writable Nucleus Area
PLPA	Pageable Link Pack Area
PSA	Prefix Storage Area
PVT	Private Area
SQA	System Queue Area
XCSA	Extended Common Storage Area above the bar
XLPVT	Extended Private Storage Area above the bar

ZSECNODE: zSecure Server nodes

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
			•	•	•	•

The `ZSECNODE NEWLIST (NEWLIST TYPE=ZSECNODE)` provides information about the zSecure Server obtained from the zSecure Address space.

Field descriptions

You can use the following fields to select and create audit reports for the zSecure-Server configuration.

CKNSERVE_LEVEL
The packaging level of the CKNSERVE server program. The field length is 8 characters.

CKNSERVE_VRM
Shows the version, release, and modification level of the CKNSERVE Server program (`V.R.M`). The field length is 8 characters.

DEFAULT_COMPLEX
Shows the value for the complex that is used by the program, if the complex value is not specified by the user. The field length is 8 characters.

HWNAME
The hardware name (if available) where the system runs. The field length is 8 characters.

IPNAME
The system host name as specified in the zSecure Server configuration file. The following formats are accepted:

- The fully-qualified domain name is the preferred format, for example: `hostname.domain.name`
- The IPv4 format, for example: `10.0.0.1`
- The IPv6 format, for example: `fe80:0:0:0:200:f8ff:fe21:67cf`

This field is empty for those systems that can only be connected through RRSF.

IPADDRESS
The resolved IP-address of the system host name. The following formats are accepted:

- The IPv4 format, for example: `10.0.0.1`
- The IPv6 format, for example: `fe80:0:0:0:200:f8ff:fe21:67cf`

This field is empty for those systems that can only be connected through RRSF.

IPPORT
The IP port number specified for the system. This value is the port number on which the zSecure Server is listening for incoming connections. For remote systems, the `IPPORT` value represents the port number that is used to connect to the remote zSecure Server. This field is empty for those systems that can only be connected through RRSF.

LAST_CONNECT
Timestamp field that shows when the last communication from this system was received by the local zSecure Server.

LAST_CONNECT_ATTEMPT
Timestamp field that shows when the last communication attempt was made by the local zSecure server to this system.

LPARNAME
The Logical Partition name where the system runs, if available. The field length is 8 characters.

RRSFNODE
The RRSF node name for the remote system. The node name is used for sending RACF commands if the user selects RRSF for command direction.This field is empty for those systems on which RRSF is not active.

RRSF_ACTIVE
Flag field that specifies if the RRSF node is active on the current system.

RRSF_DEFINED
Flag field that signals that the RRSF node has been defined locally. If this flag value is *YES*, sending RACF commands to the RRSF node is possible. If this flag value is *NO*, the RRSF node is not defined locally. The missing definition for the RRSF node might be caused by a configuration error, or the node might be a member of a separate RRSF network.

RRSF_LOCAL
Flag field that signals that this system is the local RRSF node, or this system is part of the same multisystem RRSF node as the current system. If the RRSF node is a multisystem node and is also the current system (`zsec_local=yes`) the value for the flag is *YES* for all other systems in the same RRSF node. One of these systems might be designated as `RRSF_MAIN`. If the `MAIN` system is not included as a system in the zSecure network, the `MAIN` system might be absent.

RRSF_MAIN
Flag field that identifies the `MAIN` system in the RRSF multisystem node. The concept is like the preferred system in the zSecure node. Only one system can be assigned as `MAIN` system in an RRSF node.

RRSF_USERID
Shows the associated userid value that is used as the default for command routing and authorization on the `RRSFNODE` and a possible matching `ZSECNODE`. The value of this field is dependent on the userid that creates the report.

SMFID
Shows the SMF system id, which is the value specified for the `SID` parameter in the active `SMFPRM`*xx* member in `PARMLIB`. This value identifies SMF records and is present in storage in the `SMCASID` field. In many zSecure `NEWLIST`s, this field is called `SYSTEM`.

SYSCLONE
The `&SYSCLONE` variable that identifies a system within a SYSPLEX. The field length is 2 characters.

SYSNAME
The z/OS system name that is in the `CVTSNAME` field in memory. The value might be derived from the `SYSNAME` parameter in the active IEASYS member in PARMLIB.

SYSPLEX
This field shows the sysplex name. The field length is 8 characters.

VMUSERID
The VM guest user ID hosting the system, if available. The field length is 8 characters.

ZSECNODE
The zSecure node name that describes all systems sharing the same RACF database. The value can be compared to the RRSF node name for a multisystem node. This field is empty for those systems that can only be connected through RRSF.

ZSECSYS
The zSecure system name that describes a single system. This field is empty for those systems that can only be connected through RRSF.

ZSEC_ACTIVE
Flag field that indicates if a *remote* zSecure system (`ZSECSYS`) is connected to the

local server. *YES* indicates a current connection. *NO* indicates that the system is not currently connected. The connection might have been dropped due to inactivity.

If the zSecure system represents the local server, the value of the flag is usually *NO*. The value is *YES* if the local server needed to connect to itself, for example to process a data request from a local client.

ZSEC_LOCAL
Flag field that signals that the current zSecure system record represents the local system. Only one system in the report can have a value of *YES*.

ZSEC_PREFERRED
Flag field that signals that the zSecure system is the preferred system for this zSecure node. This flag can be YES for only a single system within a zSecure node.

ZSEC_VERIFIED
Flag field that signals that the zSecure system has been contacted, and that the verification of the system information was successful. The system does not need to be currently active, but can be contacted if needed.

Chapter 14. CKGRACF Command Language

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
		•	•			

The CKGRACF program is part of IBM Security zSecure Admin. It is used for handling Queued commands (like temporary access), revoke or resume schedules, User data fields and various other functions that require updating RACF profiles. This program is also used by IBM Security zSecure Visual.

All CKGRACF commands and command options can be abbreviated to the shortest unique prefix, with a minimum of two characters. For example, the AUTHORITY command can be abbreviated as AU. Within the USER command, the INTERVAL option can be abbreviated as IN, and the PWSET option can be abbreviated as PWS. The only command that cannot be abbreviated is the CMD command, which does not accept abbreviations of the command or the command options.

This section provides information about the syntax and use of the CKGRACF commands and also provides a command reference. For more information, select the desired topic.

String conversion in CKGRACF

In all commands, *string values* can be specified in the following ways:

- Unquoted: The string is converted to uppercase and must not contain quotes, double quotes, or backquotes.
- Quoted: The string must not contain double quotes. The value can be appended with one of the optional conversion characters listed in Table 570 on page 1500.
- Double-quoted: The string must not contain single quotes. The value can be appended with one of the optional conversion characters listed in Table 570 on page 1500.
- Backquoted: The string must not contain backquotes. The value can be appended with one of the optional conversion characters listed in Table 570 on page 1500.

Table 570 on page 1500 lists the optional string conversion characters that can be appended to string values. When a conversion character is present, the value is converted based on the specified character.

Table 570. String conversion characters

Character	Meaning
C	Keep case exact
X	Convert string from hexadecimal
none	Convert string to uppercase

Note that when mixed case password support is enabled, passwords supplied on the `PWDEFAULT PASSWORD()` and `PWSET PASSWORD()` commands are not automatically converted to uppercase. Also, password phrases supplied on `PWSET PHRASE()` are never converted to uppercase.

Number conversion in CKGRACF

In all commands, *numerical values* can be specified in the following ways:

- Unquoted: The number must be a decimal.
- Quoted, double-quoted, or backquoted: The number can be decimal, hexadecimal, or binary. The value can be appended with one of the optional conversion characters listed in Table 571.

Table 571 lists the optional number conversion characters that can be appended to numerical values. When a conversion character is present, the value is converted based on the specified character.

Table 571. Number conversion characters

Conversion Character	Meaning
B	Convert from binary
F	Convert from decimal
X	Convert from hexadecimal
none	Convert from decimal

Profile conversion in CKGRACF

In all commands the profile can be specified in the following ways:

- Unquoted: The profile is taken as is. No prefixes are added, and the profile is treated as if it were quoted.
- Quoted, double-quoted, or backquoted: The profile can be appended with one of the optional conversion characters listed in Table 572.

Table 572. Profile conversion characters

Conversion Character	Meaning
C	Keep case exact
D	Profile is discrete
G	Profile is generic
X	Convert profile from hexadecimal

Date specification in CKGRACF

In all commands, dates can be specified in the following formats:

- European format (`DDMMMYY`, `DD-MMM-YY`, `DD/MMM/YY`, `DDMMMYYYY`, `DD-MMM-YYYY`, `DD/MMM/YYYY`)
- ISO format (`YYYY-MM-DD or YYYY/MM/DD`)
- Julian-date format: (`YYDDD or YYYY/DDD`)
- To specify the current date, use the special value `TODAY`.

Two-digit years are usually considered to be an error unless the error message has specifically been suppressed at the request of the user using the SUPPRESS MSG=729 command. If the case, two-digit years are interpreted as prefixed with 19.

Command separator restrictions

To issue multiple CKGRACF commands, use the ; character (semicolon) to separate each command. The only exceptions to this syntax is when specifying CMD commands without DLM option. these commands only accept end-of-line as the end of the command. If you want to specify DEBUG flags, it is advisable to put this command before all others.

Reason keywords in CKGRACF

All commands except LIST and SHOW have a REASON keyword to log extra information along with the command itself. The syntax for the reason specification is:

`REASON(`*`reason`*`)`

where *reason* is a string. See also "String conversion in CKGRACF" on page 1499.

- A maximum of 215 characters. (See "USER" on page 1533)
- Most *reason* strings can have a maximum of 233 characters. However, a *reason* string which is part of a SCHEDULE subcommand can have a maximum of 215 characters. See "USER" on page 1533.

Note that the log string in a RACF SMF record can have a maximum of 255 characters. As a result, some parts of CKGRACF commands with more than 255 characters, notably commands with very long REASON strings, are not logged. To reduce instances of truncating CKGRACF command output in the logs, use shorter REASON strings to help limit the size of the commands to 255 characters.

JCL sample for CKGRACF

The SCKRSAMP library contains the JCL sample C2RJXCKG procedure that can be used to do a single CKGRACF run. You can use the instream CKGIN data set to pass the CKGRACF command(s) to procedure C2RCXCKG. For example, to list IBMUSER, modify the instream DD statement as shown in the following code sample.

```
//C2RJXCKG EXEC C2RCXCKG,CONFIG=C2R$PARM
//CKGIN    DD *
  LIST USER IBMUSER
```

CKGRACF command reference

The following CKGRACF command reference provides information descriptions and syntax information for all CKGRACF commands.

ACCESS

The ACCESS command determines the access of a specified user or group on a specified resource or resource profile, using the best matching generic profile available.

The ACCESS command has the following syntax:

```
ACCESS id class profile [ type ] [ REASON(reason) ]
id       A userid or groupid
class    Any resource profile class
profile  A resource profile
type     An optional profile type; see below
reason   A reason ("Reason keywords in CKGRACF" on page 1501)
```

If the profile name contains generic characters (*%&), the profile is automatically considered generic. To override this behavior, you can either specify the DISCRETE keyword, or use the D suffix notation for defining a discrete profile.

The profile *types* for CKGRACF access are listed in Table 573.

Table 573. Profile types for CKGRACF ACCESS

Profile Type	Meaning
ASIS	Profile is as-is
DISCRETE	Profile is discrete
GENERIC	Profile is generic

The ACCESS command requires access to the command profile shown in Table 574.

Table 574. Command access checks for CKGRACF ACCESS

Resource name checked	Access required
CKG.CMD.ACCESS.ALL	READ

The ACCESS command is not subject to scope checks.

Notes:

- Discrete profiles are not taken into account for the class DATASET. Only the matching generic profile is checked and shown.
- The command attempts to return the access the user has through the access list, conditional access list or UACC. It ignores Global Access Table, RACF exits, and default return code as defined in the Class Descriptor Table. It will issue a message with RACROUTE REQUEST=AUTH return codes when the RACROUTE call returned with unexpected return codes. See also “DEBUG” on page 1511.

ALLOC

This command can be used to specify file allocation options. All options except LICENSE can only be specified in the parameter string.

You can specify one or more parameters, separated by blanks or commas. The parameters are:

DD=*ddname*
This parameter is used in conjunction with TYPE=INPUT and DSN=*dsn* parameters. The ddname is the MVS DD name to use for the dynamic allocation of data set *dsn*.

DSN=*dsn*
Used in conjunction with TYPE=INPUT and DD=ddname parameters, this parameter provides value for the data set name to be dynamically allocated. The *dsn* value can be enclosed in quotes. No userid is prefixed to *dsn* if the quotes are omitted. The *dsn* value specified cannot contain a member name in parentheses, nor can it be a relative member of a generation data group.

ERRDD= *ddname*
Use this parameter to redirect the SYSTERM output to a user-specified *ddname*. This parameter can only be used as a calling parameter in the PARM keyword in JCL. It cannot be used as a command in the input file.

LICENSE= *dsn(member)*
This keyword is present for backward compatibility only. It is ignored.

OUTDD= *ddname*
Use parameter to change the print output file name to a user-specified *ddname*. This parameter can only be used as a calling parameter for the PARM keyword in JCL. It cannot be used as a command in the input file.

TEXTPIPE= *n*
This parameter is valid on the PARM string only. It can be used to ship all remote text files through a UNIX pipe.

TYPE=INPUT
This parameter is used in conjunction with the DD=ddname and DSN=*dsn* parameters. The data set name *dsn* is dynamically allocated for input, using DD name *ddname*.

AUTHORITY

The AUTHORITY command can be used to set, delete, or list a profile's multiple-authority requirement. For an explanation of the multiple-authority system, see “USER” on page 1533. If a profile has no multiple-authority setting stored in the USR field, the system-wide default is used. This default value can be listed using the SHOW CKRSITE command.

The AUTHORITY command has the following syntax:

```
AUTHORITY class profile [ action ] [ REASON(reason) ]

class      Any valid RACF class
profile    Any valid RACF profile
action     One of SINGLE, DUAL, TRIPLE, DEFAULT, or LIST; see below
reason     A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

The following table lists the actions supported:

Table 575. Actions for CKGRACF AUTHORITY

Action	Meaning
DEFAULT	Delete the profile's multiple-authority requirement; the system-wide default will prevail
DUAL	Set the profile's authority-requirement to DUAL
LIST	Show the profile's multiple-authority requirement
SINGLE	Set the profile's authority-requirement to SINGLE
TRIPLE	Set the profile's authority-requirement to TRIPLE

If no action is specified, LIST is used.

The AUTHORITY command requires access to the command profiles shown in the following table.

Table 576. Command access checks for CKGRACF AUTHORITY

Resource name checked	Access required
CKG.CMD.AUTHORITY.*class*	READ for the LIST option, UPDATE for all other options.

The AUTHORITY command is not subject to scope checks.

CKGAUTH

The CKGAUTH command can be used to set, delete, or list a profile's *internal* multiple-authority requirement.

Every one of the CKG.RAC, CKG.SCP and CKG.SCPASK profiles can contain an internal multiple-authority setting. This setting will be evaluated by the CMD command to determine the eventual multiple-authority requirement for the command as a whole. It is currently not used by the USER command.

If a profile has no internal multiple-authority setting stored in the USR field, the system-wide default is used. This default can be listed using the SHOW CKRSITE command. For additional explanation of the internal multiple-authority system, see "CMD" on page 1505 and "Racfdata profiles" on page 1568.

The CKGAUTH command has the following syntax:

```
CKGAUTH class profile [ action ] [ REASON(reason) ]

class       Any valid RACF class
profile     Any valid RACF profile
action      One of SINGLE, DUAL, TRIPLE, DEFAULT, or LIST; see below
reason      A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

The following table shows the actions supported:

Table 577. Actions for CKGRACF CKGAUTH

Action	Meaning
DEFAULT	Delete the profile's multiple-authority requirement; the system-wide default will prevail
DUAL	Set the profile's authority-requirement to DUAL
LIST	Show the profile's multiple-authority requirement

Table 577. Actions for CKGRACF CKGAUTH (continued)

Action	Meaning
SINGLE	Set the profile's authority-requirement to SINGLE
TRIPLE	Set the profile's authority-requirement to TRIPLE

If no action is specified, LIST is used.

The CKGAUTH command requires access to the command profiles shown in the following table.

Table 578. Command access checks for CKGRACF CKGAUTH

Resource name checked	Access required
CKG.CMD.CKGAUTH.*class*	READ for the LIST option, UPDATE for all other options.

The CKGAUTH command is not subject to scope checks.

CNGAUTH is an alias for the CKGAUTH command.

CMD

The CMD command is used to run or queue native RACF commands. The CMD can take the following forms:

- `CMD ASK`
- `CMD REQUEST`
- `CMD EXECUTE`

The CMD ASK and REQUEST forms use the CKGRACF defined scope and multiple-authority possibilities. See "USER" on page 1533. The CMD EXECUTE command form uses the RACF scope.

The REMOVE, CONNECT and PERMIT commands can also be reversed after a certain time period.

The CMD command has the following syntax:

```
CMD [ options ] command

options    Any CMD option; see below
command    Any valid and supported RACF command (may be continued on
           next line by a trailing +)
```

A trailing plus sign (+) is used to indicate that the RACF command is continued on the next line, called a *continuation line*. Blanks after a trailing plus sign and at the beginning of continuation lines are ignored. Significant blanks have to be placed in front of a trailing plus sign.

Table 579 shows the options available for the CMD command:

Table 579. Options for CKGRACF CMD

Option	Meaning
AT *date1*	Execute *command* at date *date1*.

Table 579. Options for CKGRACF CMD (continued)

Option	Meaning
AFTER *len*	Execute *command* after *len* days from today. This option is converted to "AT *today+len*" so after today it is still clear which day the command is to be executed.
FOR *len* LEN *len*	Apply *command* for *len* days, (maximum 500 days).
UNTIL *date2*	Apply *command* until date *date2*.
NODE(zsecnode)	A zSecure Server ZSECNODE name to route the command to.
REASON(*reason*)	A reason (See also "Reason keywords in CKGRACF" on page 1501)
DLM	The DLM keyword is followed by the rest of the CMD command surrounded by matching sequences of consecutive double quotes. The command ends with the right delimiter sequence. This delimiter can be left off the command in which case the command terminates at the end of the line.
action	A queued-command action.

If no *date1* is specified, the start date of a temporary command will be the date it is actually executed. The FOR and LEN options will cause the reversed command to be executed *len* days after this execution date. If no *date2* is specified, the command is not reversed, unless a FOR or LEN option is defined to calculate *date2*.

A command that is applied for a certain period, will try to restore the situation existent at *date1* as much as possible on *date2*.

The AT and AFTER keywords are mutually exclusive. The FOR, LEN, and UNTIL keywords are mutually exclusive as well.

The following example denotes a valid sequence of two CKGRACF commands, illustrating the use of the DLM option.

```
CMD DLM """ EXECUTE ALU SOMEUSER DATA('"SING+
LE " DOUBLE "" TEST') """ ; LIST USER SOMEUSER
```

The next example has a syntax error because its plus sign (+) character is not part of the RACF command.

```
CMD DLM " EXECUTE ALU SOMEUSER DATA('TEST') " +
; LIST USER SOMEUSER
```

The following *queued-command actions* can be specified. See "Actions on queued commands" on page 1550 for more detailed information.

ASK
REQUEST
SECOND APPROVE
SECOND DENY
SECOND HOLD
COMPLETE APPROVE
COMPLETE DENY
COMPLETE HOLD

WITHDRAW
EXECUTE

The ASK, REQUEST, SECOND, COMPLETE and WITHDRAW actions are currently only allowed with the RACF commands REMOVE, CONNECT and PERMIT.

The *action* EXECUTE runs the *command* under the current userid, with the user's own permissions. Most RACF commands and HELP can be executed in this manner. A notable exception is the RVARY command.

The default action for the CMD command is ASK.

The CMD command requires access to a command profile that includes both an *action qualifier* and the *command*. The basic format of the resource name checked is CKG.CMD.CMD.*action.command.* Action qualifiers are:

- ASK for ASK
- REQ for REQUEST and WITHDRAW
- SEC for SECOND
- CMP for COMPLETE
- EX for EXECUTE

Table 580 provides the complete list of command access checks.

Table 580. Command access checks for CKGRACF CMD

Command	Action	Resource name checked	Access required
ADDGROUP	EXECUTE	CKG.CMD.CMD.EX.ADDGROUP	UPDATE
ADDSD	EXECUTE	CKG.CMD.CMD.EX.ADDSD	UPDATE
ADDUSER	EXECUTE	CKG.CMD.CMD.EX.ADDUSER	UPDATE
ALTDSD	EXECUTE	CKG.CMD.CMD.EX.ALTDSD	UPDATE
ALTGROUP	EXECUTE	CKG.CMD.CMD.EX.ALTGROUP	UPDATE
ALTUSER	EXECUTE	CKG.CMD.CMD.EX.ALTUSER	UPDATE
CONNECT	ASK	CKG.CMD.CMD.ASK.CONNECT	UPDATE
CONNECT	COMPLETE	CKG.CMD.CMD.CMP.CONNECT	UPDATE
CONNECT	EXECUTE	CKG.CMD.CMD.EX.CONNECT	UPDATE
CONNECT	REQUEST or WITHDRAW	CKG.CMD.CMD.REQ.CONNECT	UPDATE
CONNECT	SECOND	CKG.CMD.CMD.SEC.CONNECT	UPDATE
DEFINE	EXECUTE	CKG.CMD.CMD.EX.DEFINE	UPDATE
DELDSD	ASK	CKG.CMD.CMD.ASK.DELDSD	UPDATE
DELDSD	COMPLETE	CKG.CMD.CMD.CMP.DELDSD	UPDATE
DELDSD	EXECUTE	CKG.CMD.CMD.EX.DELDSD	UPDATE
DELDSD	REQUEST or WITHDRAW	CKG.CMD.CMD.REQ.DELDSD	UPDATE
DELDSD	SECOND	CKG.CMD.CMD.SEC.DELDSD	UPDATE
DELETE	EXECUTE	CKG.CMD.CMD.EX.DELETE	UPDATE
DELGROUP	EXECUTE	CKG.CMD.CMD.EX.DELGROUP	UPDATE
DELUSER	EXECUTE	CKG.CMD.CMD.EX.DELUSER	UPDATE

Table 580. Command access checks for CKGRACF CMD (continued)

Command	Action	Resource name checked	Access required
HELP	EXECUTE	CKG.CMD.CMD.EX.HELP	READ
LISTDSD	EXECUTE	CKG.CMD.CMD.EX.LISTDSD	READ
LISTGRP	EXECUTE	CKG.CMD.CMD.EX.LISTGRP	READ
LISTUSER	EXECUTE	CKG.CMD.CMD.EX.LISTUSER	READ
PASSWORD	EXECUTE	CKG.CMD.CMD.EX.PASSWORD	UPDATE
PERMIT	ASK	CKG.CMD.CMD.ASK.PERMIT	UPDATE
PERMIT	COMPLETE	CKG.CMD.CMD.CMP.PERMIT	UPDATE
PERMIT	EXECUTE	CKG.CMD.CMD.EX.PERMIT	UPDATE
PERMIT	REQUEST or WITHDRAW	CKG.CMD.CMD.REQ.PERMIT	UPDATE
PERMIT	SECOND	CKG.CMD.CMD.SEC.PERMIT	UPDATE
RACDCERT	EXECUTE	CKG.CMD.CMD.EX.RACDCERT	UPDATE
RACLINK	EXECUTE	CKG.CMD.CMD.EX.RACLINK	UPDATE
RACMAP	EXECUTE	CKG.CMD.CMD.EX.RACMAP	UPDATE
RALTER	EXECUTE	CKG.CMD.CMD.EX.RALTER	UPDATE
RDEFINE	EXECUTE	CKG.CMD.CMD.EX.RDEFINE	UPDATE
RDELETE	ASK	CKG.CMD.CMD.ASK.RDELETE	UPDATE
RDELETE	COMPLETE	CKG.CMD.CMD.CMP.RDELETE	UPDATE
RDELETE	EXECUTE	CKG.CMD.CMD.EX.RDELETE	UPDATE
RDELETE	REQUEST or WITHDRAW	CKG.CMD.CMD.REQ.RDELETE	UPDATE
RDELETE	SECOND	CKG.CMD.CMD.SEC.RDELETE	UPDATE
REMOVE	ASK	CKG.CMD.CMD.ASK.REMOVE	UPDATE
REMOVE	COMPLETE	CKG.CMD.CMD.CMP.REMOVE	UPDATE
REMOVE	EXECUTE	CKG.CMD.CMD.EX.REMOVE	UPDATE
REMOVE	REQUEST or WITHDRAW	CKG.CMD.CMD.REQ.REMOVE	UPDATE
REMOVE	SECOND	CKG.CMD.CMD.SEC.REMOVE	UPDATE
RLIST	EXECUTE	CKG.CMD.CMD.EX.RLIST	READ
SEARCH	EXECUTE	CKG.CMD.CMD.EX.SEARCH	READ
SETROPTS	EXECUTE	CKG.CMD.CMD.EX.SETROPTS	UPDATE

In addition, the target profile must be within the `racfdata-scope` of the command user. See "CKGRACF authority checks" on page 1559 and "Racfdata profiles" on page 1568.

Table 581. Racfdata scope checks for CKGRACF CMD

Resource name checked	Access required
CKG.RAC.OWN.*class.segment.field*	READ for LIST commands; UPDATE for all other options.
CKG.RAC.ALL.*class.segment.field*	READ for LIST commands; UPDATE for all other options.

Table 581. Racfdata scope checks for CKGRACF CMD (continued)

Resource name checked	Access required
CKG.RAC.SCP.*class.segment.field*	READ fo LIST commands; UPDATE for all other options.
CKG.SCP.ID.*userid.owner.dfltgrp*	READ for LIST commands; UPDATE for all other options.
CKG.SCP.ID.*groupid.owner*	READ for LIST commands; UPDATE for all other options.
CKG.SCP.G.*groups...*	READ for LIST commands; UPDATE for all other options.
CKG.SCP.U.*user.groups...*	READ for LIST commands; UPDATE for all other options.
CKG.SCPASK.ID.*userid.owner.dfltgrp*	READ for LIST commands; UPDATE for all other options.
CKG.SCPASK.ID.*groupid.owner*	READ for LIST commands; UPDATE for all other options.
CKG.SCPASK.G.*groups...*	READ for LIST commands; UPDATE for all other options.
CKG.SCPASK.U.*user.groups...*	READ for LIST commands; UPDATE for all other options.

Every one of the CKG.RAC, CKG.SCP and CKG.SCPASK profiles can contain an internal multiple-authority setting. This setting will be evaluated by the CMD command to determine the eventual multiple-authority requirement for the command as a whole.

The actual multiple-authority requirement for the command will be the highest of the multiple-authority requirement set on the target profile, and the internal multiple-authority requirements set on the CKG.RAC, CKG.SCP and CKG.SCPASK profiles.

The internal multiple-authority requirement for a profile can be set using the CKGAUTH command. See "CKGAUTH" on page 1504).

Warning about passwords

Depending on the audit level of the CKG.CMD.CMD profile, RACF commands issued through CMD or USER PWSET can be logged in SMF and written to the job output if CKGRACF is run in batch. These commands can show passwords and password phrases.

When a PASSWORD or PHRASE parameter is recognized in a RACF command, the secret value is replaced by a question mark. To prevent password collection from the SMF or the job log, make sure that the PASSWORD or PHRASE parameter is not abbreviated to fewer than 4 positions and that the left parenthesis is coded immediately following the parameter with no spaces. The following examples shows the logging for different formats:

`ALTUSER IBMUSER PASS(1234)` is logged as `ALTUSER IBMUSER PASS(?)` with no password displayed.

`ALTUSER IBMUSER PAS(1234)` is logged as-is to SMF, displaying the password.

`ALTUSER IBMUSER PASSWORD (1234)` includes a blank before the opening parenthesis and is logged as-is, displaying the password.

Comments

A few comments regarding the supported RACF commands;

- For the PERMIT and DELDSD commands, the DATASET profiles are prepended with the TSO-prefix, if it is available, and then put in quotes before queueing. If the DATASET is already enclosed with quotes, this does not apply.
- The *action* REQUEST can be abbreviated to REQ, SECOND can be abbreviated to SEC, COMPLETE can be abbreviated to CMP and EXECUTE can be abbreviated to EX or EXEC.
- The target for scope checking and storing of a queued command is chosen as logical as possible. For CONNECT and REMOVE this is the GROUP they act on; This to ensure that on deletion of the GROUP all related queued commands will be purged, too. For DELDSD, PERMIT, and RDELETE commands, it is the resource the command pertains to. This will also assure the purging of all related queued commands on deletion of the resource.

Restrictions

The following restrictions apply to the CMD command:

- The CMD *options* can not be abbreviated
- RVARY is not supported by EXECUTE.
- CONNECT, DELDSD, PERMIT, RDELETE, and REMOVE are the only supported RACF commands for ASK and REQUEST.
- The PERMIT command only supports a single userid and a single access definition for temporary commands (commands with an UNTIL date, or a LEN or FOR period defined).
- The CONNECT and REMOVE commands only support a single userid.
- The PERMIT command doesn't support the FROM parameter for a temporary command.
- CONNECT, PERMIT and REMOVE will restore the situation that exists at execution when UNTIL, FOR or LEN is specified.
- DELDSD and RDELETE cannot be combined with UNTIL, FOR, and LEN.
- The RACF command parser ignores characters between a semicolon and the end of the line. A CMD command can therefore only be followed by a ; command separator and another CKGRACF command on the same line if its RACF subcommand is delimited using the DLM option.

COMMENT

This command basically does nothing at all. It gets logged as any other normal CKGRACF command and only accepts one parameter; REASON (See also “Reason keywords in CKGRACF” on page 1501). This command can be used to log a comment in between other commands.

The COMMENT command has the following syntax:

```
COMMENT [ REASON(reason) ]
reason      A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

The COMMENT command requires access to the command profiles shown in the following table.

Table 582. Command access checks for CKGRACF COMMENT

Resource name checked	Access required
CKG.CMD.COMMENT	READ

The COMMENT command is not subject to scope checks.

DEBUG

This command is meant to explore the working of CKGRACF or diagnose problems in its operation. It should not be used in any application visible to end-users. If you need additional details, contact IBM software support.

You can specify one or more parameters after the DEBUG command, separated by blanks or commas. The parameters are:

ICHEINTY
Print the ICHEINTY return code, reason code, and a short explanation after each failed ICHEINTY call. Message numbers CKG407I, CKG408I, and CKG409I. See the 'Security Server RACF Macros and Interfaces' manual for additional information on the ICHEINTY result codes.

RACFMSG
Do not inhibit RACF messages, for example make all RACROUTE REQUEST=AUTH calls with MSGSUPP=NO instead of the CKGRACF default MSGSUPP=YES. This results in ICH408I and other messages being printed in the job log and system log. See the 'Security Server RACF Messages and Codes' manual for additional information on the RACF messages.

RACHECK
Print the resource name and access level checked before each RACROUTE REQUEST=AUTH call, and the profile name found after each call. The message numbers are CKG402I and CKG410I.

SAFRC
Print the SAF return code, RACF return code, and RACF reason code after each RACROUTE call. The message also gives a rough indication of the request type. Message numbers CKG401I, CKG403I, CKG404I, CKG405I, and CKG406I. See the 'Security Server RACROUTE Macro Reference' manual, in the section indicated by the request code, for additional information on the RACROUTE result codes.

The DEBUG command does not require access to command profiles and is not subject to scope checks.

FIELD

The FIELD command can be used to set or list a limited number of fields in user profiles that cannot be set by the RACF commands. It is intended for use by system programmers and (central) RACF administrators.

The FIELD command has the following syntax:

```
FIELD class profile action field(value) ... [ REASON(reason) ]

class                     Must be USER.
profile                   Any valid RACF userid.
action                    One of ADD, DELETE, LIST, REPLACE, or SET.
field                     The name of a supported field, possibly
field(value)              followed by one or more field-values
field(old-value,new-value) in parentheses, see the table below.
reason                    A reason (Reason keywords in CKGRACF)
```

A field *value* can be specified as a string, quotes and conversions are allowed. The field *action* determines whether a field value is allowed, according to the following table.

Table 583. Actions for CKGRACF FIELD

Action	Values	Effect	Example
ADD	one	Set the field to the value	ADD TCOMMAND(MYCLIST)
DELETE	none	Set the field to its default value	DELETE TCOMMAND
DELETE	one	Set the field to its default value if the current value matches the parameter	DELETE TCOMMAND(MYCLIST)
LIST	none	List the field	LIST LJDATE
REPLACE	two	Replace the value of the field if the current value matches the parameter	REPLACE TCOMMAND(OCLIST,NCLIST)
SET	one	Set the field to the value	SET TCOMMAND(MYCLIST)

More than one field can be specified in a single FIELD command, but each field can be specified at most once; the same action will be applied to each of the fields in turn. If an error occurs with one of the specified actions, the others will still be processed and might change the profile.

Warning: If an invalid value (or format) id used to set or replace, or if you delete the value of a field, problems can occur.

The FIELD command requires an exact specification of the field in a format that matches the RACF internal representation of the field value. For instance, the TCOMMAND field is a character field, and thus the CKGRACF FIELD command expects the input value to be in character format (or hexadecimal representation thereof). On the other hand, the LJDATE and PASSDATE fields each have a packed decimal value. The only supported way of specifying such a value is via its hexadecimal representation as 'yydddF'x. For LJDATE and PASSDATE, the first character (2 hex digits) specifies the year value, while ddd specifies the julian date. The "F" at the end represents the sign ("F" is defined for Packed Decimal to represent a positive number). A year character between '71'x and '99'x denotes a year in the 20th century, while a year character between '00'x and '70'x denotes a year in the 21th century. For example, '71'x denotes 1971 while '00'x denotes 2000.

The following table summarizes the required formats.

Table 584. Fields for CKGRACF FIELD

Name	Meaning	Length	Format
BINDPW	PROXY segment Bind password	Variable, up to 128 characters	'xxxx...xx'x
BINDPWKY	PROXY segment Bind password mask or encrypt key	71	'xxxx...xx'x
FLAG7	Password or password phrase needed	1	'nn'x
FLAG8	OIDCARD required	1	'nn'x

Table 584. Fields for CKGRACF FIELD (continued)

Name	Meaning	Length	Format
INTERVAL	Password and password phrase interval	1	'nn'x
LJDATE	Last-use date	3	'yydddF'x
LJTIME	Last-use time	4 .	'hhmmsscc'x
PASSASIS	Password mixed case	1	'nn'x
PASSDATE	Password change date	3	'yydddF'x
PASSWORD	Encrypted password	8	'xxxxxxxxxxxxxxxx'x
PHRASE	Encrypted pass phrase	Variable, up to 100 characters	'xxxx...xx'x
PHRDATE	Pass phrase change date	3	'yydddF'x
REVOKECT	Revoke counter	1	'nn'x
SSKEY	SSIGNON segment Session key	Variable, up to 255 characters	'xxxx...xx'x
SESSKEY	SESSION segment Session key	Variable, up to 8 characters	'xxxx...xx'x
TCOMMAND	TSO start-up command	Variable, up to 80 characters	'quoted string' or unquoted_string
TUPT	TSO UPT data	Variable, up to 255 characters	'xxxx...xx'x

Changing the PASSDATE or PHRDATE field while running RRSF causes the last use date/time and the last connect date/time to be updated to a time dependent on the response time of RRSF.

The TCOMMAND and TUPT fields are intended to be used for SYS1.UADS to RACF migration; the LJDATE, LJTIME, PHRASE, PASSWORD, INTERVAL, PASSDATE, PHRDATE and REVOKECT fields can be used when merging RACF databases. Security zSecure also generates CKGRACF commands to update the TCOMMAND field. The length specified in the preceding table must match the length of the value supplied to the FIELD command; if the length is different, an error message is issued.

Notes:

1. In the restructured database, adding a TCOMMAND or TUPT field creates a TSO segment if the profile does not have one yet.
2. If the LJDATE field is set to an invalid date, RACF might abend when the user attempts to logon or when a LISTUSER command is executed.
3. If the INTERVAL field is set to 0, then a user must change his password at each logon.
4. The FIELD command requires access to the command profiles listed in Table 585. The access required is different for different fields.

Table 585. Command access checks for CKGRACF FIELD

Field	Resource name checked	Access required
INTERVAL	CKG.CMD.FIELD.INTERVAL	READ for the LIST option, UPDATE for all other options.
LJDATE	CKG.CMD.FIELD.LJDATE	READ for the LIST option, UPDATE for all other options.

Table 585. Command access checks for CKGRACF FIELD (continued)

Field	Resource name checked	Access required
LJTIME	CKG.CMD.FIELD.LJTIME	READ for the LIST option, UPDATE for all other options.
PASSASIS	CKG.CMD.FIELD.PASSASIS	READ for the LIST option, UPDATE for all other options.
PASSDATE	CKG.CMD.FIELD.PASSDATE	READ for the LIST option, UPDATE for all other options.
PASSWORD	CKG.CMD.FIELD.PASSWORD (See "Note about password-related fields.")	READ for the LIST option, UPDATE for all other options.
PHRASE	CKG.CMD.FIELD.PHRASE (See "Note about password-related fields.")	READ for the LIST option, UPDATE for all other options.
PHRDATE	CKG.CMD.FIELD.PHRDATE	READ for the LIST option, UPDATE for all other options.
REVOKECT	CKG.CMD.FIELD.REVOKECT	READ for the LIST option, UPDATE for all other options.
TCOMMAND	CKG.CMD.FIELD.TCOMMAND	READ for the LIST option, UPDATE for all other options.
TUPT	CKG.CMD.FIELD.TUPT	READ for the LIST option, UPDATE for all other options.
FLAG7	CKG.CMD.FIELD.FLAG7	READ for the LIST option, UPDATE for all other options.
FLAG8	CKG.CMD.FIELD.FLAG8	READ for the LIST option, UPDATE for all other options.

Note:

The FIELD command is not subject to scope checks. Because the PASSWORD and PHRASE fields can be used to list all users' encrypted password information, make sure that access to the field is restricted. Access to these fields should be only be granted to users who are also allowed to read the active RACF database in unrestricted mode.

Example

An example of the FIELD command is taken from the RECREATE USER CARLa script (member CKGXRUS in the SCKRCARL library). The CARLa commands in this script generate CKGRACF FIELD commands to recreate the user's password, TSO command, and TSO UPT data fields. To recreate the user's password, a RACF database is required. The following excerpt of CKGXRUS shows CARLa commands to generate CKGRACF FIELD commands to recreate the user's TSO UPT data fields.

```
new nopage f=ckrcmd nulls proflist=users name=ckgtupt    /*QZ0607003*/
  s likelist=idsel s=tso exists(tupt)                    /*QZ0607003*/
  sortlist 'ckgracf field' class key(8) 'set',
           "tupt('" | tupt(hex,0) | "'X)"
```

Part of CARLa script CKGXRUS

The following sample output command is generated by Security zSecure.

```
ckgracf field USER R#OPADM
set tupt('00380000000000000000000001000001D97BD6D7D9D6C207C5D5E4C5D5E40'X)
```

Sample CKGRACF FIELD command generated by Security zSecure

IMBED / INCLUDE

The IMBED or INCLUDE command (abbreviation: I) can be used to include input commands for CKGRACF from a different source than the program/command parameters and the SYSIN file. The INCLUDE commands can be nested, for example, the input commands included can contain another include command. The main use of this command is to include sample or user-defined members or read commands from a file; this can be used to share queries or output displays. Using the INCLUDE command to include a standard installation-defined member is a simple customization option.

The commands are read immediately after the INCLUDE statement ends. After the secondary input source has been exhausted, processing of the original input source is resumed at the token that terminated the INCLUDE statement. The input listing clearly shows the origin of the input commands.

The parameters are:

DDNAME= *file* **FILE=***file*
To imbed the contents of a sequential file or (in combination with the MEMBER parameter) to denote the file containing the member to be imbedded. If MEMBER is specified as well, a partitioned data set (concatenation) must be allocated to the file.

MEMBER= *name*
To imbed the contents of a PDS member. If the DDNAME parameter is also present, the PDS allocated to that file is used. If the DDNAME parameter is omitted, the DDname CKRCARLA is assumed.

MARGINS= *(nn,ll)* **MARGINS(***nn,ll***)**
Set the margins for the included file or member. The default is dependent on the input LRECL and RECFM. For an LRECL=80 RECFM=F file, this results in a default of MARGINS(1,72).

The IMBED command does not require access to command profiles.

LIST

The LIST command can be used to display RACF as well as CKGRACF data and settings for a profile. The CKGRACF settings are stored in the USR field of a profile, and have a USRNM value starting with the characters CNG; the LIST command is used to display USR entries that cannot be set or displayed using the USRDATA command. The CKGRACF settings for a profile can include:

- The profile's multiple-authority requirement (for all profiles)
- Queued commands that have the profile as their target (for all profiles)
- A user's default password (for a user) [22]
- Scheduled revoke and resume actions (for a user)

22. The LIST command indicates that a default password was set; also, when and by whom it was set. The default password is not displayed.

For auditing purposes, the LIST command displays the author, date, and time for each setting.

The LIST command also displays the index (USRNM-value) of unknown reserved USR entries.

Listing the RACF settings is only possible for class USER, and will include (non-exhaustive):

- Last connect/login date and time
- Group access list
- Default group
- Revoke status of user
- PROTECTED attribute
- RESTRICTED attribute

The LIST command has the following syntax:

```
LIST class profile [ option ]
class     Any valid RACF class
profile   Any valid RACF profile
option    One of ALL, RACF, SCHEDULE, TAG [ NOTERM ] [ NOPAGE ] or QUEUE;
see below
```

The following table shows the options supported:

Table 586. Options for CKGRACF LIST

Option	Meaning
ALL	List all RACF and CKGRACF data
RACF	List the RACF data
SCHEDULE	List scheduled resume and revoke actions
TAG [NOTERM] [NOPAGE]	List profile's data in tagged format (See below)
QUEUE	List queued CKGRACF commands

If no option is specified, ALL is used for USER and QUEUE for all other classes.

When the TAG option is followed by NOTERM, the output of the LIST command is not sent to SYSTERM. This can save bandwidth e.g. when the output is transferred from one machine to another. When the NOPAGE option is present, no page headers will be printed between the tagged format lines. This simplifies parsing the output.

The LIST command requires access to the command profile shown in the following table.

Table 587. Command access checks for CKGRACF LIST

Resource name checked	Access required
CKG.CMD.LIST	READ

In addition, the target user must be within the scope of the command user (see "CKGRACF authority checks" on page 1559):

Table 588. Scope access checks for CKGRACF LIST

Resource name checked	Access required
CKG.SCP.ID.*groupid.owner*	READ
CKG.SCP.ID.*userid.owner.dlftgrp*	READ
CKG.SCP.G.*groups...*	READ
CKG.SCP.U.*user.groups...*	READ

Example

```
CKGRACF LIST USER C##CX01

------------ Status of USER C##CX01 on 23Aug2006 08:57 at IPO1 -------------
--------------------------- Inactive PwdExpired ----------------------------
Last use date:     26Sep2003 15:26:43.59
Last connect date: 12Mar1999 13:13:17.49

Username             RIRP SOA Created   PwChanged/Int/Try Owner    Dfltgrp
TEST USER, NO TSO    -I-- --- 02Feb1996 Expired    30   0 CR##     CR##
PERSONNEL NUMBER 1234567890

Groupname Auth R SOA AG T Uacc Connected Instdata
>CR##     USE  - --- -- N NONE 02Feb1996 EXTERNAL USERS
 C##CXGRP USE  - --- -- N NONE 10Feb2000 GROUP TO TEST 1 GROUP SPECIAL USER
 C##CXDEL USE  - --- -- N NONE 16Feb2000 TEST GROUP FOR DEVELOPMENT

CKG112I 00 No CKGRACF-reserved userdata entries found
CKG132I 00 No CKGRACF queued command entries found
CKG133I 00 No CKGRACF schedule data entries found
```

Sample output of the LIST command

TAG Format

The TAG option for the LIST command generates a machine readable output with a very specific syntax. Every line of output is defined as follows:

```
X-field verbose value(s)

X         A profile type identifier for field (See below)
field     A RACF field name or a likely other name
verbose   A more verbose description or name for field
value     The value that is stored in field
```

The identifier can have different values for different fields: 'C' for CKGRACF related fields, 'G' for GROUP, 'U' for USER, 'R' for GENERAL RESOURCE, 'D' for DATA SET, 'S' for SCHEDULE information (See also “USER” on page 1533), 'Q' for queued command information (See also “CMD” on page 1505) and 'I' for generic information.

The field *field* has a fixed length of 8 (10 including the indicator) and is right padded with spaces. The field *verbose* has a fixed length of 16 (right padded with spaces). Every non-empty line starting with a space, is a continuation of the previous line. If *value* is a list of other values (for example in a repeat group), the list items will be separated by spaces. If the *values* are strings, every list element will be shown on a new line, starting with a space as described before. Any newline (X'15') character in *value* will be printed as a space if the LIST TAG output is sent to a text pipe. Otherwise, it will be printed as a newline.

A few definitions: string is defined as a series of characters and whitespaces. An integer is defined as a number within the mentioned range. A date is defined as

DDMMMYYYY, where MMM is the month as a three character abbreviation (eg. Mar for March). A time is defined as HH:MM:SS.cc, where HH is hours from 0-23, MM is minutes from 0-59, SS is seconds from 0-59 and cc is hundredths of seconds from 0-99. A queued command stamp is defined as an action, followed by a time stamp of the form USERID DDMMMYYYY HH:MM. An action can contain whitespace.

Table 589. User related fields for CKGRACF LIST

Field	Verbose	Value	Description
U-AUTH	AUTHORITY	CONNECT, CREATE, JOIN, or USE	The authority of the user to the group
U-AUTHDATE	CREATIONDATE	A date (DDMMMYYYY)	The date this user is created
U-AUTHOR	OWNER	A userid or groupid	The owner of the user profile
U-AUTHOR	CONNECTAUTHOR	A userid or groupid	The author of the connect
U-CATEGORY	CATEGORIES	Any number of categories (strings)	A list of all the categories this user can access
U-CLAUTH	CLASSAUTHS	Any number of 8 character classes	A list of all the classes this user can access
U-CONUSRNM	USER	A userid	The userid of a user connected to a group
U-DFLTGRP	DEFAULTGROUP	A groupid	The default group of this user
U-EXPIRED	PASSWORD_EXPIRED	Y or N	Password or password phrase (if any) has expired
U-FLAG1	ADSP	Y or N	The ADSP setting of a user
U-FLAG2	SPECIAL	Y or N	The SPECIAL setting of a user
U-FLAG3	OPERATIONS	Y or N	The OPERATIONS setting of a user
U-FLAG4	REVOKE	Y or N	Whether a user is revoked or not
U-FLAG5	GRPACC	Y or N	The GRPACC setting of a user
U-FLAG6	AUDITOR	Y or N	The AUDITOR setting of a user
U-GRPREVOK	CONNECTREVOKE	Y or N	Whether the user has the REVOKE attribute in the connect group entry. The revoke date, resume date, and REVOKE attribute of the connect group entry are taken into account.
U-CGREVKDT	CONNECTREVOKEDT	Date (DDMMMYYYY)	The revoke date for the connect group entry.
U-CGRESMDT	CONNECTRESUMEDT	Date (DDMMMYYYY)	The resume date for the connect group entry.
U-INACTIVE	REVOKEINACTIVE	INACTIVE or ACTIVE	With INACTIVE the user will be revoked on next logon

Table 589. User related fields for CKGRACF LIST (continued)

Field	Verbose	Value	Description
U-INSTDATA	INSTALLATIONDATA	A string	The installation data of this user
U-LCDATE	LASTCONNECTDATE	A date (DDMMMYYYY)	The date a user has last connected to a group
U-LCTIME	LASTCONNECTTIME	A time (HH:MM:SS.cc)	The time a user has last connected to a group
U-LJDATE	LASTLOGINDATE	A date (DDMMMYYYY)	The date a user has last logged on
U-LJTIME	LASTLOGINTIME	A time (HH:MM:SS.cc)	The time a user has last logged on
U-LOGDAYS	LOGDAYS	S or space, M or space, T or space, W or space, T or space, F or space, and S or space	The days of the week the user can log on
U-NOTRMUAC	NOTERMUACC	Y or N	The user must be authorized with at least READ authority to access a terminal.
U-PASSCHG	PASSWORD_CHANGED	A date (DDMMMYYYY) or empty	The last date this user's password has been changed. It is empty if the password has expired. Also see the U-PHRCHG and U-PASSDATE fields.
U-PASSDATE	PWDLASTCHANGED	A date (DDMMMYYYY) or empty	The last date this user's password or password phrase has been changed. This field is empty if both the password and password phrase have expired. Also, see the U-PASSCHANGE and U-PHRCHG fields.
U-PASSINT	PWDINTERVAL	An integer (0-255), or empty (for a PROTECTED user)	The number of days within which a password or password phrase has to be changed.
U-PGMRNAME	USERNAME	A string	The user's name as stored in PGMRNAME.
U-PHRCHG	PHRASE_CHANGED	A date (DDMMMYYYY) or empty	The last date this user's password phrase has been changed. The field is empty if the password phrase has expired, or the user has no password phrase. (See also U-PASSCHG and U-PASSDT fields.)
U-PROTECT	PROTECTED	Y or N	The PROTECTED setting of a user.
U-RESTRICT	RESTRICTED	Y or N	The RESTRICTED setting of a user.

Table 589. User related fields for CKGRACF LIST (continued)

Field	Verbose	Value	Description
U-REVOKE	REVOKESTATUS	REVOKED or NOT REVOKED	Whether a user is revoked by date.
U-REVOKECT	PWDTRIES	An integer (0-255)	The number of invalid passwords or password phrase attempts since the last logon.
U-SECLABEL	SECLABEL	A string	The security label of this user.
U-SECLEVEL	SECLEVEL	An integer (0-255)	The security level of this user.
U-UACC	CONNECTUACC	ALTER, CONTROL, UPDATE, READ, EXECUTE, or NONE	The default universal access authority assigned to the user for this group.

Table 590. Group related fields for CKGRACF LIST

Field	Verbose	Value	Description
G-AUTH	AUTHORITY	One of the connect authority levels	The authority the user has for this group.
G-AUTHDATE	CREATIONDATE	A date (DDMMMYYYY)	The date the connect from the user to this group was created.
G-AUTHOR	OWNER	A groupid or userid	The owner of this group.
G-CAUTHOR	CONNECTAUTHOR	A groupid or userid	The owner of this connect.
G-CONGRPNM	GROUPNAME	A string	The name of this group.
G-FLAG1	ADSP	Y or N	The ADSP setting of the user for this group.
G-FLAG2	SPECIAL	Y or N	The SPECIAL setting of the user for this group.
G-FLAG3	OPERATIONS	Y or N	The OPERATIONS setting of the user for this group.
G-FLAG5	GRPACC	Y or N	The GRPACC setting of the user for this group.
G-FLAG6	AUDITOR	Y or N	The AUDITOR setting of the user for this group.
G-GRPREVOK	CONNECTREVOKE	Y or N	Whether the user has the REVOKE attribute in the connect group entry. The revoke date, resume date, and REVOKE attribute of the connect group entry are taken into account.
G-CGREVKDT	CONNECTREVOKEDT	Date (DDMMMYYYY)	The revoke date for the connect group entry.
G-CGRESMDT	CONNECTRESUMEDT	Date (DDMMMYYYY)	The resume date for the connect group entry.
G-INSTDATA	INSTALLATIONDATA	A string	The installation data for this connect or group.

Table 590. Group related fields for CKGRACF LIST (continued)

Field	Verbose	Value	Description
G-LJDATE	LASTCONNECTDATE	A date (DDMMMYYYY)	The date the user has last connected to this group.
G-LJTIME	LASTCONNECTTIME	A time (HH:MM:SS.cc)	The time the user has last connected to this group.
G-NOTRMUAC	NOTERMUACC	Y or N	The NOTERMUAC setting of the user for this group.
G-SUBGRPNM	GROUPNAME	A groupid	The name of a subgroup.
G-SUPGROUP	SUPERIORGROUP	A groupid	The superior group to this group.
G-UACC	UACC	CONNECT, CREATE, JOIN, or USE	The universal group authority.
G-UNVFLG	UNIVERSAL	Y or N	The group is UNIVERSAL.

Table 591. General resource related fields for CKGRACF LIST

Field	Verbose	Value	Description
R-AUDITF	AUDITFAILURE	ALTER, CONTROL, UPDATE, or READ	Global audit FAILURES qualifier.
R-AUDITS	AUDITSUCCESS	ALTER, CONTROL, UPDATE, or READ	Global audit SUCCESS qualifier.
R-DEFDATE	DEFINITIONDATE	A date (DDMMMYYYY)	The date the resource was defined to RACF.
R-INSTDATA	INSTALLATIONDATA	A string	Installation data of the resource.
R-NOTIFY	NOTIFY	A userid	The user to be notified when access violations occur against the resource protected by this profile.
R-AUTHOR	OWNER	A groupid or userid	The owner of the resource.
R-SECLABEL	SECURITYLABEL	A string	The security label of the resource.
R-UACC	UNIVERSALACCESS	ALTER, CONTROL, UPDATE, READ, EXECUTE, or NONE	The universal access authority for the resource.
R-WARNING	WARNING	Y or N	The data set has the WARNING attribute.

Table 592. Data set related fields for CKGRACF LIST

Field	Verbose	Value	Description
D-AUTHOR	OWNER	A groupid or userid	The owner of the data set.
D-UACC	UNIVERSALACCESS	ALTER, CONTROL, UPDATE, READ, EXECUTE, or NONE	The universal access authority for the data set.

Table 593. CKGRACF related fields for CKGRACF LIST

Field	Verbose	Value	Description
C-AUTHORIT	CNGMULTIPLEAUTH	SINGLE, DUAL or TRIPLE	The CKGRACF multiple authority set on this profile.
C-CNGAUTH	CNGINTERNMULTAUT	SINGLE, DUAL or TRIPLE	The internal multiple authority setting for this profile.
C-PWDFLT	CNGPWDEFAULT	A stamp	Stamp to show who set a default password at what time.
Q-ACTION	LASTACTION	One of the queued command actions	The last action performed on this queued command.
Q-CMD	QUEUEDCOMMAND	A string	The actual queued command.
Q-CMDSTMP1	COMMANDSTAMP1	A queued command stamp (See above)	A stamp to show what user did what action.
Q-CMDSTMP2	COMMANDSTAMP2	A queued command stamp (See above)	A stamp to show what user did what action.
Q-CMDSTMP3	COMMANDSTAMP3	A queued command stamp (See above)	A stamp to show what user did what action.
Q-CMDSTMP4	COMMANDSTAMP4	A queued command stamp (See above)	A stamp to show what user did what action.
Q-CMDSTMP5	COMMANDSTAMP5	A queued command stamp (See above)	A stamp to show what user did what action.

For schedule entries in a USER profile, the format of output is slightly different. For every schedule, the *field* name contains the name of the schedule and the identifier is an 'S'. The *verbose* field contains a definition of the contents of the value field. A list of possible combinations follows. A line S-*name* SCHEDULE is a marker for a specific part of a schedule. Any REASON, DELETED or DELREASON *verbose* fields following that line, are associated with that specific part of the schedule.

The I-SCHEDULE SUMMARY lines contain the summarized schedule, considering all schedule entries and their result (See also “USER” on page 1533).

Table 594. Schedule related fields for CKGRACF LIST

Field	Verbose	Value	Description
S-*name*	SCHEDULE	A schedule entry	Gives information about schedule *name*.
S-*name*	REASON	A string	Gives the reason for schedule *name*.
S-*name*	DELETED	A time stamp	The current part of schedule *name* has been deleted.
S-*name*	DELREASON	A string	Gives the reason for DELETED.
I-SCHEDULE	SUMMARY	A string	Summarizes all schedules and their effects.

PWCONVERT

The PWCONVERT command converts a password of a user that was encrypted using the masking algorithm to the installation's encryption method (presumably DES). This can be used as one of the final steps in the elimination of masked passwords.

The PWCONVERT command works in the following manner:

- The user's password is decrypted using the masking algorithm. This always succeeds. For a password encrypted with the masking algorithm, the correct password is found. For passwords encrypted with another method (e.g. DES), an incorrect, nonsense, password is found.
- If the decrypted password seems likely (for example, it can be entered from a keyboard), it is encrypted using the installation's encryption method, and it is saved. Otherwise, the conversion fails.

The PWCONVERT command can be used to limit the duration of a password migration period, when the installation is using the password migration option of the RACF password-encryption exit ICHDEX01 or ICHDEX11. If this option is used, passwords are encrypted and verified using both DES and masking encryption. The migration period should be limited to a short period of time, since it introduces the remote possibility of a *false positive*: a password encrypted using DES that is also the result of a different password encrypted using the masking algorithm. This different password could also be used to logon. In the case of a false positive, the PWCONVERT command gives a wrong result, since it converts the different (wrong) password to the new encryption method.

The PWCONVERT command has the following syntax:

```
PWCONVERT userid [ REASON(reason) ]
userid    Any valid RACF userid.
reason    A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

Userids that have passwords encrypted using the masking algorithm can be detected with the PWHASHED field in the Security zSecure `RACF NEWLIST`. The CARLa script CKRLPWHC can be used to detect all userids with hashed passwords and generate CKGRACF commands to convert the passwords. Note that the PWHASHED field is subject to the same chance of a mistake as the PWCONVERT command.

The PWCONVERT command requires access to the command profile shown in the following table.

Table 595. Command access checks for CKGRACF PWCONVERT

Resource name checked	Access required
CKG.CMD.PWCONVERT	UPDATE

In addition, the command user must have system-wide SPECIAL authority. The PWCONVERT command is not subject to scope checks.

QUESTION

The QUESTION command can be used to set, delete, or verify question/answer pairs, and to list questions present in a user profile.

The QUESTION command has the following syntax:

```
QUESTION profile [ REASON(reason) ] SET qid question PASSWORD(answer) ...
QUESTION profile [ REASON(reason) ] VERIFY qid PASSWORD(answer) ...
QUESTION profile [ REASON(reason) ] LIST [ qid ] ...
QUESTION profile [ REASON(reason) ] DELETE [ qid ] ...

profile           Any valid RACF profile in the USER class
qid               A question identifier, which has syntax Qnn where nn
                  is a nonnegative integer below 100. A question identifier
                  provides an index to a single question/answer pair.
reason            A reason string ("Reason keywords in CKGRACF" on page 1501)
```

Each *question* and *answer* value must be specified as a string (where quotes and conversions are allowed). The *action* (SET, VERIFY, LIST, or DELETE) determines the number of question identifiers that can be specified. The next table presents the details.

Table 596. Actions for CKGRACF QUESTION

Action	Number	Effect	Example
DELETE	none	Deletes all previous question/answer pairs, if present.	DELETE
DELETE	one or more	For each *qid*, deletes the previous question/answer pair identified by *qid*, if present.	DELETE *qid*
LIST	none	Lists all previous question/answer pairs, if present.	LIST
LIST	one or more	For each *qid*, lists the previous question/answer pair identified by *qid*, if present.	LIST *qid*
SET	one or more	For each *qid*, deletes the previous question/answer pair identified by *qid*, if present; then adds a question/answer pair identified by *qid*	SET *qid question* PASSWORD(*answer*)
VERIFY	one or more	For each *qid*, verifies whether the current answer matches with the previous answer identified by *qid*.	VERIFY *qid* PASSWORD(*answer*)

More than one question identifier (+ question + answer) can be specified in a single QUESTION command; the same action is applied to each identifier (+ question + answer) in turn. The target profile is not changed if an error occurs within a single QUESTION command.

The QUESTION command requires access to the command profile shown in the following table.

Table 597. Command access checks for CKGRACF QUESTION

Resource name checked	Access required
CKG.CMD.QUESTION	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.

In addition, the target user must be within the userdata-scope of the command user (see "CKGRACF authority checks" on page 1559). In the following table, each *nn* is a two-digit number corresponding with question identifier Q*nn*.

Table 598. USRDATA access checks for CKGRACF QUESTION

Resource name checked	Access required
CKG.USRDATA.OWN.USER.CNGC2H*nn*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.
CKG.USRDATA.ALL.USER.CNGC2H*nn*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.
CKG.USRDATA.SCP.USER.CNGC2H*nn*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.

If access to CKG.USRDATA.SCP.USER.CNGC2H*nn* is defined, the following profiles will be checked:

Table 599. Scope access checks for CKGRACF QUESTION

Resource name checked	Access required
CKG.SCP.ID.*userid.owner.dfltgrp*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.
CKG.SCP.ID.*groupid.owner*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.
CKG.SCP.G.*groups...*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.
CKG.SCP.U.*user.groups...*	READ for the LIST and VERIFY actions; UPDATE for the SET and DELETE actions.

Restrictions

A QUESTION command accesses the USR field of a user profile. There are several restrictions on the use of the USR field and the QUESTION command:

- The Security zSecure RECREATE command does not recreate the full USR field. It recreates the multiple-authority setting and installation-defined entries.
- The Security zSecure COPY command does not copy USR fields.

Representation of question/answer pairs

A question/answer pair is represented as an entry in the USR field of a user profile. The USRNM field of the entry is of the form CNGC2H*nn* where *nn* is a two-digit number corresponding with the question identifier Q*nn* of the question/answer pair. The *data* of the USR field entry (for example, the value of the USRDATA field of the entry) consists of a question and a hashed answer. The answer is hashed in such a way that it is very difficult to find another answer with the same hash. The value of the corresponding USRFLG field indicates which hash method has been used. A value of 0 indicates a 16 byte MD5 hash of the concatenation of the answer and the userid.

RDELETE

The RDELETE command can be used to delete any RACF data set, general profile, user profile, or group profile. This can be used for the following purposes:

- Delete fully-qualified generics in general resource classes
- Delete profiles that contain lowercase characters
- Delete data set profiles with the name of a temporary data set, e.g. SYS88308....
- Delete discrete profiles that contain generic characters
- Delete profiles of a group with a zero superior group field.

The RDELETE command cannot be used to delete CONNECT profiles.

The RDELETE command has the following syntax:

```
RDELETE class profile [ type ] [ volser ] [ REASON(reason) ]
class     Any RACF class except CONNECT.
profile   Any profile name; see below.
type      An optional profile type; see below.
volser    An optional volume serial.
reason    A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

The profile can be specified with profile conversion characters (See also “Profile conversion in CKGRACF” on page 1500).

The profile *type* can be one of the following:

Table 600. Profile types for CKGRACF RDELETE

Type	Meaning
ASIS	Profile is as-is
DISCRETE	Profile is discrete
GENERIC	Profile is generic

If no profile type has been specified, and the conversion characters 'C' or 'D' have been used, the conversion characters are used. If neither has been used, the default is ASIS. If both are used, an error message is issued.

If you are generating the CKGRACF to delete the offending profiles with e.g., a CARLa RACF NEWLISTRACF query that selects them, we recommend that you use the field HEXKEY to print the profile name in hexadecimal with the profile conversion character X.

Note: For USER, GROUP, and DATASET profiles, the full name must be specified. Unquoted data set profiles are *not* prefixed with the user's TSO prefix.

Also note that connections to or from users and groups are not deleted when a user or group profile is deleted with RDELETE.

The RDELETE command requires access to the command profile shown in the table below:

Table 601. Command access checks for CKGRACF RDELETE

Resource name checked	Access required
CKG.CMD.RDELETE	UPDATE

In addition, the command user must have system-wide SPECIAL authority. The RDELETE command is not subject to scope checks.

Example - delete a discrete profile with generic characters

For example, assume you have created profile SYS* in class FACILITY, while generic processing was disabled. A discrete profile was created. Now, generic processing is enabled, and you want to delete the profile without disturbing the system in its operation. You can delete the profile with the following command:

```
CKGRACF RDELETE FACILITY 'SYS*' DISCRETE
or
CKGRACF RDELETE FACILITY 'SYS*'D
```

Example - delete a profile with nonprintables, via CARLa

A good way to get rid of *funny* profiles, especially when they contain non-printables, is to use a CARLa query. The recommended approach is as follows.

1. Use the following query (from the ISPF interface, e.g., option **CO.C**, is easiest) with a rough selection that includes the offending profile and displays the DB and RBA fields, which together uniquely identify a specific profile/segment within the database.

   ```
   n t='Select the problem profile in the RACF DB',
     name=SELPROF
     x not(segment=base)
     <step 1): insert rough select statement here>
     <step 2): replace rough select by precise select on DB/RBA>
     sortlist db rba class segment key(44 wrap),
              proftype volume hexkey(0 wrap)
   ```

2. Replace the rough selection with a selection for only the offending profile. We recommend using the DB and RBA values of the offending profile.
3. Add the following (chained) NEWLIST to generate a CKGRACF RDELETE command to CKRCMD.

   ```
   n t='Generate CKGRACF RDEL with the exact HEX key of the profile',
     dd=ckrcmd nopage
     select LISTLIKE=SELPROF
     sortlist "ckgracf rdel" class(0) "'" | hexkey(0) | "'X",
            / "/*  " proftype volume key(44 wrap) "*/"
   ```

4. Verify that the only the offending profile has been selected now. Run the generated CKGRACF RDELETE command.

Note: If you ran the query from the ISPF interface, you can press <PF3> after verification and then use 'R' before CKRCMD in the RESULTS panel to run the generated CKGRACF RDELETE command (because of dd=ckrcmd).

REFRESH

The REFRESH command can be used to update a user profile's revoke/resume settings and to execute or expire queued commands. As a result of a REFRESH command, the user's revoke status and revoke and resume dates can be changed as a scheduled revoke/resume setting is applied. (Note that the USER SCHEDULE and USER RESUME commands immediately apply any changes required; a REFRESH is needed to apply *delayed* settings at the appropriate date.)

The REFRESH command has the following syntax:

```
REFRESH class profile [ REASON(reason) ]

class      Any valid RACF class
profile    Any valid RACF profile
reason     A reason (See also "Reason keywords in CKGRACF" on page 1501)
```

The REFRESH command requires access to the command profile shown in the following table.

Table 602. Command access checks for CKGRACF REFRESH

Resource name checked	Access required
CKG.CMD.REFRESH	UPDATE

The REFRESH command is not subject to scope checks.

The need for a refresh

The following types of CKGRACF commands require a RACF action to be carried out at a future date:

- Queued commands that expire or must be deleted
- Scheduled revoke/resume settings that must be replaced
- Pending commands that need to be executed

Since CKGRACF does not alter the operation of RACF, these actions do not occur of themselves. Instead, CKGRACF must be called with the REFRESH command to perform the relevant actions. When CKGRACF is called to REFRESH a profile, the following actions are performed:

- Queued commands that have expired are marked 'expired'.
- Expired or completed queued commands that have been kept beyond the auditing period are deleted.
- If the resume date of a scheduled revoke or resume setting has passed, and a future set of revoke and resume dates has been scheduled, the revoke and resume date are replaced.
- Inactive scheduled revoke and resume actions that have been kept beyond the auditing period are deleted from the schedule.
- Pending commands are executed and reversed if needed. A pending command will be executed if the planned date for execution is today or already past, and the command still falls within the time period determined by the AT and UNTIL/FOR/LEN keywords.

If a REFRESH is not performed, the following effects occur:

- An expired queued command that has not been marked 'expired' is expired if a user performs any action on the queued command. The queued command cannot be approved, denied, or held.
- If the resume date of a revoke/resume period has passed since the last REFRESH command, and a future revoke/resume period has been scheduled, these future settings are not applied. As a result, the current revoke/resume period is maintained. If a REFRESH is late by one or two days, but occurs at any time between the end of one revoke/resume period and the start of another, the next scheduled revoke/resume dates will be applied properly. Only if no REFRESH is performed at all until after the next revoke/resume date, the user will not have been revoked or resumed in time.
- Queued commands and scheduled revoke/resume settings that have been kept beyond the auditing period are not deleted until the next refresh.
- A pending command is not executed. It will either expire in case of a temporary command (A command that only needs to be 'active' for a certain time), or it will be executed belatedly at the first refresh (which can be very undesirable)

The Security zSecure query CKGXREFR has been provided to determine the user profiles that require a REFRESH. You are advised to run this query as part of a daily job. The query generates the required CKGRACF REFRESH commands. If the daily job is not executed or fails for some reason, the next query can result in delayed REFRESH commands being generated; in the interim period, the effects noted in preceding paragraphs can occur. It is advisable to run the refresh job early each day, to ensure the timely execution of queued commands.

Example: Refreshing a timed command: On the 12th of January, the following command is given:
CKGRACF CMD AT 20JAN2003 FOR 1 PE MY.** ID(HER) ACCESS(READ)

The daily refresh job runs each night just after midnight. The refresh at 20JAN2003 (at for example one minute past midnight) will grant READ access to HER, through the execution of PE MY.** ID(HER) ACCESS(READ). The refresh at 21JAN2003 will restore the situation of 20JAN2003. (For example by issuing PE MY.** ID(HER) DELETE or PE MY.** ID(HER) ACCESS(UPDATE) depending on whether HER already had access and if so, what level.)

If in this example, the 20JAN2003 refresh run is not executed, this user will not get access to MY.** and the command will be expired at 21JAN2003.

Example

An example of the REFRESH command is taken from a CARLa script that generates REFRESH commands for those profiles that need a refresh (member CKGXREFR in the CARLa library).

```
newlist name=REFRGEN  f=CKGOUT nopage title='Refresh generic profiles'
select ckgrefresh<today generic
sortlist "refresh" class "'" | key(0) | "'g"
newlist name=REFRREST f=CKGOUT nopage title='Refresh other profiles'
select ckgrefresh<today not(generic)
sortlist "refresh" class "'" | key(0) | "'d"
```

Part of CARLa script CKGXREFR

SHOW

The SHOW command can be used to show the settings configured in the CKRSITE module or to show a user's access to certain resources.

The SHOW command has the following syntax:

```
SHOW option
```

where `option` can contain any of the option values listed in Table 603.

Table 603. Options for CKGRACF SHOW

Option	Meaning
CKRSITE	Show settings configured in the CKRSITE module.
MYACCESS [NOTERM]	Show the access of the issuer of the command to certain profiles.
MYACCESS ID *id* [NOTERM]	Show the access of userid or groupid to certain profiles.
ZAP	This is an alias for CKRSITE.

The SHOW CKRSITE command shows the settings configured in the CKRSITE module. This command is executed immediately during input parsing (most other commands are delayed until all the commands have been parsed successfully). It prints message CKG100I and shows the class used for profile checks, the default authority requirement for the USER command, the command expiration period, and the auditing expiration period.

The SHOW CKRSITE command does not require access to command profiles and is not subject to scope checks.

Both SHOW MYACCESS and SHOW MYACCESS ID *id* report a number of lines of the following form:

```
resource name access level profile name or possibly empty message

resource name     One of the resource names listed below
access level      NONE, READ, UPDATE, CONTROL, or ALTER
profile name      The profile which determines the access to the resource
```

A message "*userid* has been revoked" will be printed instead of a profile name if *userid* has been revoked. In this case, the access level is set to NONE. In some cases, an empty message is printed instead of a profile name. In these cases, the access level is set to NONE and a separate CKG*nnn*I message is printed.

SHOW MYACCESS shows the access the user has through the access list, conditional access list or UACC. It ignores Global Access Table, RACF exits, and default return code as defined in the Class Descriptor Table.

Access to the following command profile related resources will be reported by CKGRACF SHOW MYACCESS [id]:

C2R.SERVER.ADMIN
CKG.CMD.CMD.EX.ADDGROUP
CKG.CMD.CMD.EX.ADDSD
CKG.CMD.CMD.EX.ADDUSER
CKG.CMD.CMD.EX.ALTDSD
CKG.CMD.CMD.EX.ALTGROUP
CKG.CMD.CMD.EX.ALTUSER
CKG.CMD.CMD.EX.CKGRACF
CKG.CMD.CMD.EX.DELDSD
CKG.CMD.CMD.EX.DELGROUP
CKG.CMD.CMD.EX.PERMIT
CKG.CMD.CMD.EX.RACMAP
CKG.CMD.CMD.EX.RALTER
CKG.CMD.CMD.EX.RDEFINE
CKG.CMD.CMD.EX.RDELETE
CKG.CMD.CMD.EX.SETROPTS
CKG.CMD.CMD.REQ.CONNECT
CKG.CMD.CMD.REQ.PERMIT
CKG.CMD.CMD.REQ.REMOVE
CKG.CMD.LIST
CKG.CMD.USER.REQ.INTERVAL
CKG.CMD.USER.REQ.NOINTERVAL
CKG.CMD.USER.REQ.PWDEFAULT
CKG.CMD.USER.REQ.PWNOEXIT
CKG.CMD.USER.REQ.PWNOHIST
CKG.CMD.USER.REQ.PWNORULE
CKG.CMD.USER.REQ.PWRESET

CKG.CMD.USER.REQ.PWSET
CKG.CMD.USER.REQ.PWSET.*
CKG.CMD.USER.REQ.PWSET.PASSWORD
CKG.CMD.USER.REQ.PWSET.PROMPT
CKG.CMD.USER.REQ.PWSET.DEFAULT
CKG.CMD.USER.REQ.PWSET.PREVIOUS
CKG.CMD.USER.REQ.PWSET.NOPASSWD
CKG.CMD.USER.REQ.PWSET.CURRENT
CKG.CMD.USER.REQ.PWSET.EXPIRED
CKG.CMD.USER.REQ.PWSET.NONEXP
CKG.CMD.USER.REQ.RESUME
CKG.CMD.USER.REQ.SCHEDULE
CKG.RAC.SCP.CONNECT.BASE.SPECIAL
CKG.RAC.SCP.CONNECT.BASE.OPERATIO
CKG.RAC.SCP.CONNECT.BASE.AUDITOR
CKG.RAC.SCP.CONNECT.BASE.OWNER
CKG.RAC.SCP.CONNECT.BASE.RESUME
CKG.RAC.SCP.CONNECT.BASE.REVOKE
CKG.RAC.SCP.CONNECT.BASE.AUTH.USE
CKG.RAC.SCP.CONNECT.BASE.AUTH.CREATE
CKG.RAC.SCP.CONNECT.BASE.AUTH.JOIN
CKG.RAC.SCP.CONNECT.BASE.AUTH.CONN
CKG.RAC.ALL.CONNECT.BASE.SPECIAL
CKG.RAC.ALL.CONNECT.BASE.OPERATIO
CKG.RAC.ALL.CONNECT.BASE.AUDITOR
CKG.RAC.ALL.CONNECT.BASE.OWNER
CKG.RAC.ALL.CONNECT.BASE.RESUME
CKG.RAC.ALL.CONNECT.BASE.REVOKE
CKG.RAC.ALL.CONNECT.BASE.AUTH.USE
CKG.RAC.ALL.CONNECT.BASE.AUTH.CREATE
CKG.RAC.ALL.CONNECT.BASE.AUTH.JOIN
CKG.RAC.ALL.CONNECT.BASE.AUTH.CONN

Additionally, access to discrete profiles of the form CKG.SCHEDULE.*name*, of the form CKG.CMD.CKGAUTH.*name*, or starting with CKG.UCAT. will be reported. For each such profile in the database, there will be one corresponding line in the report. Generic schedule profiles are not reported.

The SHOW MYACCESS command (without ID id) requires access to the following command profile.

Table 604. Command access checks for CKGRACF SHOW MYACCESS

Resource name checked	Access required
CKG.CMD.SHOW.MYACCESS	READ

The SHOW MYACCESS ID *id* command requires access to the following command profiles.

Table 605. Command access checks for CKGRACF SHOW MYACCESS ID id

Resource name checked	Access required
CKG.CMD.ACCESS.ALL	READ
CKG.CMD.SHOW.MYACCESS	READ

When SHOW MYACCESS [ID *id*] is followed by the NOTERM option, the output is not sent to SYSTERM.

Example - SHOW CKRSITE

```
CKGRACF SHOW CKRSITE
CKG100I 00 Contents of CKRSITE module:
           Class:              XFACILIT
           Authority:          SINGLE
           Command expiration: 7
           Audit expiration:   30
```

The meaning of the options listed is:

- The class checked for CKGRACF profiles is XFACILIT. Thus, when the manual refers to 'command resource name CKG.CMD.REFRESH', the XFACILIT class is checked for a profile matching that resource name.
- The default multiple-authority setting is SINGLE. This means that any user that does not have a multiple-authority requirement of his own is subject to single authority. Other options are DUAL and TRIPLE.
- The command expiration time is 7 days. This means that a queued command must be acted upon within 7 days of the previous action. After 7 days, the queued command expires and can no longer be executed.
- The audit expiration time is 30 days. This means that completed or expired commands, and scheduled actions which are wiped or which are not effective anymore will be deleted after 30 days. Until that time, the completed commands and wiped scheduled actions can be displayed using the LIST USER command.

Verify that these options are the same in the Security zSecure program. The Security zSecure command SHOW CKRSITE can be used to display those settings.

SUPPRESS

The SUPPRESS command can be used to suppress messages by number. The command has a global scope and applies to all commands.

The command has the following parameters:

MESSAGE= list
MSG=*list*

A single message number or a list of message numbers enclosed in parentheses. Specifying number *nnn* suppresses message CKG*nnn*I;*nnn* must be in the range 0 to 999. Besides suppressing the messages, this parameter also suppresses processing of the return code associated with the message. Therefore, most serious error messages are not suppressed. Use this option to suppress messages inherent to your configuration that you know about but do not want to clutter your output with on each run.

The SUPPRESS command does not require access to command profiles and is not subject to scope checks.

Example - suppress messages

The following example shows how to suppress error messages you have seen often enough. The example assumes you want to suppress CKG272I and CKG273I.

```
SUPPRESS MSG=(272,273)
```

USER

The USER command can be used for central and decentral user maintenance. It is subject to the multiple-authority settings as well as revoke and resume actions use schedules. Both multiple-authority settings and schedules are explained in this section.

The USER command has the following syntax:

```
USER userid subcommand ...  [ action ] [ REASON(reason) ]
     userid Any valid RACF userid.
 subcommand A USER subcommand; see below; one or more different
            subcommands may be specified.
 action     A queued-command action; see below; the default, REQUEST,
            performs the command for a single-authority userid.
 reason     A reason string (See "Reason keywords in CKGRACF" on page 1501).
```

Specifying USER subcommands

A single USER command can include multiple subcommands. Some subcommands are mutually exclusive. If an error occurs in any of the subcommands when the USER command is processed, the target profile is not changed.

The following *subcommands* can be specified.

- INTERVAL(*value*)
- NOINTERVAL
- PWDEFAULT [*password-option*]
- PWNOEXIT
- PWNOHIST
- PWNORULE
- PWRESET
- PWSET [*password-option*] [*expired-option*]
- RACLINK UNDEF[(*node.id*)]
- RESUME
- SCHEDULE*scheduleaction* [*date*] [*reason*]

See “USER subcommands” on page 1536 for more information about each subcommand.

Specifying Queued-command actions

The USER command requires access to a command profile that includes both an *action qualifier* and the command option. The basic format of the resource name checked is CKG.CMD.USER.*action.option.*. You can specify the following values for action.option:

- ASK for ASK
- REQ for REQUEST
- WITHDRAW
- SEC for SECOND
- CMP for COMPLETE.

If no queued-command action is specified, REQUEST is used. If SECOND or COMPLETE is specified without further qualification, APPROVE is used.

When a queued command is re-entered for a stage following REQUEST, the following processing occurs:

- The PROMPT option does not prompt again.
- The password specified with the PASSWORD option is ignored.
- The REASON keyword is ignored.

The following *queued-command actions* can be specified for CKGRACF USER. See Actions on queued commands for information on these actions.

ASK
REQUEST
SECOND APPROVE
SECOND DENY
SECOND HOLD
COMPLETEAPPROVE
COMPLETE
COMPLETE DENY
COMPLETE HOLD
WITHDRAW

Access checking

The type of access checking done for a USER command depends on the options specified on the command. See the following topics for more information.

- "Access checks for options of CKGRACF USER PWSET"
- "Scope access checks for CKGRACF USER" on page 1536
- "Schedule access checks for CKGRACF USER SCHEDULE" on page 1536

Access checks for options of CKGRACF USER PWSET: The PWSET option can also have several sub-options. For backwards compatibility, the PWSET option alone includes all sub-options in the command profile check. Therefore, for profile checking, the CKG.CMD.USER.*action.*PWSET command is effectively the same as the CKG.CMD.USER.*action.*PWSET.* command for checking.

A full list of checks is shown in the following table.

Table 606. Command access checks for options of CKGRACF USER PWSET

USER PWSET Option	Actions	Resource name checked	Access required
INTERVAL	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.INTERVAL CKG.CMD.USER.REQ.INTERVAL CKG.CMD.USER.SEC.INTERVAL CKG.CMD.USER.SEC.INTERVAL CKG.CMD.USER.CMP.INTERVAL	UPDATE
NOINTERVAL	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.NOINTERVAL CKG.CMD.USER.REQ.NOINTERVAL CKG.CMD.USER.SEC.NOINTERVAL CKG.CMD.USER.CMP.NOINTERVAL	UPDATE

Table 606. Command access checks for options of CKGRACF USER PWSET (continued)

USER PWSET Option	Actions	Resource name checked	Access required
PWDEFAULT	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWDEFAULT CKG.CMD.USER.REQ.PWDEFAULT CKG.CMD.USER.SEC.PWDEFAULT CKG.CMD.USER.CMP.PWDEFAULT	UPDATE
PWNOEXIT	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWNOEXIT CKG.CMD.USER.REQ.PWNOEXIT CKG.CMD.USER.SEC.PWNOEXIT CKG.CMD.USER.CMP.PWNOEXIT	UPDATE
PWNOHIST	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWNOHIST CKG.CMD.USER.REQ.PWNOHIST CKG.CMD.USER.SEC.PWNOHIST CKG.CMD.USER.CMP.PWNOHIST	UPDATE
PWNORULE	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWNORULE CKG.CMD.USER.REQ.PWNORULE CKG.CMD.USER.SEC.PWNORULE CKG.CMD.USER.CMP.PWNORULE	UPDATE
PWRESET	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWRESET CKG.CMD.USER.REQ.PWRESET CKG.CMD.USER.SEC.PWRESET CKG.CMD.USER.CMP.PWRESET	UPDATE
PWSET	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET CKG.CMD.USER.REQ.PWSET CKG.CMD.USER.SEC.PWSET CKG.CMD.USER.CMP.PWSET	UPDATE
PWSET PASSWORD	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET.PASSWORD CKG.CMD.USER.REQ.PWSET.PASSWORD CKG.CMD.USER.SEC.PWSET.PASSWORD CKG.CMD.USER.CMP.PWSET,PASSWORD	UPDATE
PWSET PROMPT	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET.PROMPT CKG.CMD.USER.REQ.PWSET.PROMPT CKG.CMD.USER.SEC.PWSET.PROMPT CKG.CMD.USER.CMP.PWSET.PROMPT	UPDATE
PWSET DEFAULT	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET.DEFAULT CKG.CMD.USER.REQ.PWSET.DEFAULT CKG.CMD.USER.SEC.PWSET.DEFAULT CKG.CMD.USER.CMP.PWSET.DEFAULT	UPDATE
PWSET PREVIOUS	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET.PREVIOUS CKG.CMD.USER.REQ.PWSET.PREVIOUS CKG.CMD.USER.SEC.PWSET.PREVIOUS CKG.CMD.USER.CMP.PWSET.PREVIOUS	UPDATE
PWSET NOPASSWORD	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET NOPASSWORD CKG.CMD.USER.REQ.PWSET NOPASSWORD CKG.CMD.USER.SEC.PWSET NOPASSWORD CKG.CMD.USER.CMP.PWSET NOPASSWORD	UPDATE
PWSET RANDOM	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET RANDOM CKG.CMD.USER.REQ.PWSET RANDOM CKG.CMD.USER.SEC.PWSET RANDOM CKG.CMD.USER.CMP.PWSET RANDOM	UPDATE

Table 606. Command access checks for options of CKGRACF USER PWSET (continued)

USER PWSET Option	Actions	Resource name checked	Access required
PWSET CURRENT	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET CURRENT CKG.CMD.USER.REQ.PWSET CURRENT CKG.CMD.USER.SEC.PWSET CURRENT CKG.CMD.USER.CMP.PWSET CURRENT	UPDATE
PWSET EXPIRED	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET EXPIRED CKG.CMD.USER.REQ.PWSET EXPIRED CKG.CMD.USER.SEC.PWSET EXPIRED CKG.CMD.USER.CMP.PWSET EXPIRED	UPDATE
PWSET NONEXPIRED	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET NONEXPIRED CKG.CMD.USER.REQ.PWSET NONEXPIRED CKG.CMD.USER.SEC.PWSET NONEXPIRED CKG.CMD.USER.CMP.PWSET NONEXPIRED	UPDATE
PWSET PHRASE	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.PWSET PHRASE CKG.CMD.USER.REQ.PWSET PHRASE CKG.CMD.USER.SEC.PWSET PHRASE CKG.CMD.USER.CMP.PWSET PHRASE	UPDATE
RESUME	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.RESUME CKG.CMD.USER.REQ.RESUME CKG.CMD.USER.SEC.RESUME CKG.CMD.USER.CMP.RESUME	UPDATE
SCHEDULE	ASK REQUEST or WITHDRAW SECOND COMPLETE	CKG.CMD.USER.ASK.SCHEDULE CKG.CMD.USER.REQ.SCHEDULE CKG.CMD.USER.SEC.SCHEDULE CKG.CMD.USER.CMP.SCHEDULE	UPDATE

Scope access checks for CKGRACF USER: In addition to access checking for the USER PWSET options, the target user must be within the scope of the command user. (See CKGRACF authority checks.)

Table 607. Scope access checks for CKGRACF USER

Resource name checked	Access required
CKG.SCP.ID.*userid.owner.dlftgrp*	UPDATE
CKG.SCP.G.*groups...*	UPDATE
CKG.SCP.U.*user.groups...*	UPDATE

Schedule access checks for CKGRACF USER SCHEDULE: For a USER SCHEDULE command, the user must have access to the target schedule:

Table 608. Schedule access checks for CKGRACF USER SCHEDULE

Resource name checked	Access required
CKG.SCHEDULE.*schedule*	UPDATE

USER subcommands

This section describes the subcommands supported by the USER command.

INTERVAL: The INTERVAL subcommand can be used to set the password and password phrase interval for a user. If this value is lower than the system-wide interval setting, then it becomes the effective interval setting. Otherwise, the value

from the system-wide interval setting is used. The user's password and password phrase (if any) are not affected. The INTERVAL subcommand is mutually exclusive with the NOINTERVAL subcommand.

The INTERVAL subcommand has the following syntax:

```
INTERVAL[(value)]
value      A value of at least one and at most the system's INTERVAL value
(due to SETROPTS PASSWORD(INTERVAL), or 254 if no system
INTERVAL value was set).  If value is not specified, the SETROPTS
value will be taken.
```

NOINTERVAL : The NOINTERVAL subcommand can be used to turn off a user's password and password phrase interval so that no password or password phrase change is required. The user's password and password phrase (if any) are not affected. The NOINTERVAL subcommand is mutually exclusive with the INTERVAL subcommand.

The NOINTERVAL subcommand has no parameters It has the following syntax:

```
NOINTERVAL
```

PWDEFAULT: The PWDEFAULT subcommand can be used to set or delete a user's default password. This password is used when the PWRESET or PWSET DEFAULT commands are used. The default password is subject to the password rules, password history, and new-password exit at the time of setting, and is stored in encrypted form.

The PWDEFAULT subcommand has the following syntax:

```
PWDEFAULT [ password-option ]
password-option   Any PWDEFAULT password option; see below.
```

Table 609 list the PWDEFAULT password options.

Table 609. Options for CKGRACF USER PWDEFAULT

Option	Meaning
DELETE	Delete the default password, if present.
PASSWORD*(value)*	Set the default password to *value* (*value* is the password in clear text). The parentheses and the value are optional if the action is not REQUEST.
PROMPT	Prompt and re-prompt for a default password. This option cannot be used in batch mode.

If no password-option is specified, and the program is not in batch mode, PROMPT is used. In batch mode, an error message is issued.

If the target userid is subject to multiple-authority controls, the default password as specified with the REQUEST action is used. For subsequent action, use either the PASSWORD option with a dummy password, or use the PROMPT option. You are not prompted again.

If the default password is set while mixed case password support is inactive, and a password is reset (using CKGRACF) while mixed case password support is active, you might need to enter your password in uppercase to be able to logon.

If the USER PWDEFAULT and either the USER PWSET or the USER PWRESET subcommands are used in a single USER command, the PWDEFAULT subcommand is executed before the PWSET or PWRESET subcommand.

PWNOEXIT: The PWNOEXIT subcommand can be used to disable the ICHPWX01 exit call from CKGRACF when a password is set with PWSET, for example, and to disable the ICHPWX11 exit call from CKGRACF when a password phrase is set. This subcommand is useless on its own, since it's only valid for the current USER command.

The PWNOEXIT subcommand has no parameters; it has the following syntax:

```
PWNOEXIT
```

PWNOHIST: The PWNOHIST subcommand can be used to disable the history check performed by CKGRACF when a password or password phrase is set with PWSET, for example. This subcommand is useless on its own, since it's only valid for the current USER command.

The PWNOHIST subcommand has no parameters; it has the following syntax:

```
PWNOHIST
```

PWNORULE: The PWNORULE subcommand can be used to disable the password and password phrase rule checking performed by CKGRACF when a password or password phrase is set withPWSET, for example. This subcommand is useless on its own, since it's only valid for the current USER command.

PWRESET: The PWRESET subcommand can be used to set the user's password to the user's default password as set by CKGRACF. Its function is identical to PWSET DEFAULT EXPIRED. This option is provided as a relatively safe option for a helpdesk, while the PWSET option should be restricted.

The PWRESET subcommand has no parameters; it has the following syntax:

```
PWRESET
```

The PWRESET subcommand is mutually exclusive with the PWSET subcommand.

If the target user is subject to multiple-authority controls, the default password at the time of the REQUEST action is used. Changes to the default password while the command is queued do not change the copy of the default password stored with the queued command. If the default password was changed during queueing, warning message CKG646I is to be issued when the command is completed. If no default password can be found, the PWSET subcommand fails; the user is not prompted for a password.

If the default password is set while mixed case password support is inactive, and a password is reset (using CKGRACF) while mixed case password support is active, you might need to enter your password in uppercase to be able to logon.

If the PWDEFAULT and PWRESET subcommands are used in a single USER command, the PWDEFAULT subcommand is executed before the PWRESET subcommand.

PWSET: The PWSET subcommand can be used to set a user's password or password phrase.

It has the following syntax:

```
PWSET password-option expire-option
password-option   Any PWSET password option; see below.
expire-option     Any PWSET expire option; see below.
```

The PWSET subcommand is mutually exclusive with the PWRESET subcommand.

The PWSET password options are:

Table 610. Options for CKGRACF USER PWSET

Option	Meaning
PASSWORD*(value)*	Set the password to *value*, which is the password in clear text. The parentheses and value are optional if the action is not REQUEST.
PHRASE*(value)*	Set the password phrase to *value*, which is the password phrase in clear text, enclosed in single quotes. A single quote in the password phrase must be written as two consecutive single quotes, so a phrase like `th'is'phrase` must be specified as `'th''is''phrase'`. The parentheses and value are optional if the action is not REQUEST.
PROMPT	Prompt and re-prompt for a password. This option cannot be used in batch mode.
DEFAULT	Set the password to the default password.
RANDOM	Set the password to a random string. See section “Creating random passwords” on page 1553.
NOPASSWORD	Sets the status of the userid to protected, so it cannot be used to enter the system by employing a password or password phrase. See section “Protecting a userid with the PWSET NOPASSWORD option” on page 1554.
PREVIOUS	Return to the previous password from the password history. This might not be the actual previous password, for example, if the ALTUSER command has been used or if the current password has been zapped. The current password is added to the password history; thus, repeated use of the PWSET PREVIOUS subcommand alternates between two passwords, and does not travel back through the whole of the password history.
CURRENT	Leaves the password unchanged. This option is intended to be used with expire option EXPIRED or NONEXPIRED to expire or unexpire the current password phrase. The password history and the password phrase history is not read or changed.

If no password option is specified, DEFAULT is used. If no default password can be found, the user is prompted for a password. A new password specified for the PASSWORD or PROMPT options, or a prompted password for the DEFAULT option, is subject to the password rules, the password history, and the new-password exit.

When the default password is set while mixed case password support is inactive, and a password is reset (using CKGRACF) while mixed case password support is active, you might need to enter your password in uppercase to be able to logon.

If the PWDEFAULT and PWSET DEFAULT subcommands are used in a single USER command, the PWDEFAULT subcommand is executed before the PWSET subcommand.

If the target userid is subject to multiple-authority controls, the password or password phrase as read or specified in the REQUEST action is used. For subsequent actions, the PASSWORD option can be used with a dummy password or password phrase, and the PROMPT option does not prompt again. Changes to the default password while a PWSET DEFAULT subcommand is queued do not change the copy of the default password stored with the queued command; similarly, changes to the previous password while a PWSET PREVIOUS subcommand is queued do not change the copy of the previous password stored with the queued command. In both cases, warning message CKG645I or CKG646I is issued when the command is completed.

The PWSET expire options are:

Table 611. Expire options for CKGRACF USER PWSET

Option	Meaning
EXPIRED	Expire the new password or password phrase; it must be changed at the next logon.
NONEXPIRED	Do not expire the new password or password phrase.

If no expire option is specified, EXPIRED is used.

RACLINK UNDEF: Use the `RACLINK UNDEF` subcommand for deleting (undefining) all associations of a user. You can use the `RACLINK UNDEF(`*`node.id`*`)` subcommand for deleting a single association, between the user on the node where the subcommand is executed–the local node–and the user ID on node *node*. This command is designed to remove the one-sided association left when a `TSO RACLINK UNDEF` operation refuses to delete either the reference of *user1* to *user2*, or the reference of *user2* to *user1*.

Unlike the `TSO RACLINK UNDEF` command, the `RACLINK UNDEF(`*`node.id`*`)` subcommand does not remove the reference to the local user from the user profile on the remote node *node*. Indiscriminate use of the `RACLINK UNDEF` subcommand can therefore lead to inconsistencies in user associations.

RESUME: The RESUME subcommand can be used to resume a user. The current revoke/resume schedules for the user (as set by the USER SCHEDULE command) are taken into account; if these determine the user's revoke/resume status, they will be applied. If no scheduled revoke/resume actions are present, or if all scheduled actions apply to future dates, the RESUME subcommand resumes the userid. The RESUME subcommand can be used to override the revoke status as set by the ALTUSER REVOKE command, or due to excessive logon attempts or inactivity.

If the scheduled actions determine that the user should be revoked, the RESUME subcommand sets the userid to revoked status and issues message CKG120I.

In addition to setting the revoke status and the revoke/resume dates, the RESUME subcommand always sets the last-use date and time to midnight (00:00) of today, and sets the revoke count (which counts faulty password and password phrase attempts) to zero. This ensures that, by the time the user is resumed (either now or

when the scheduled resume date is reached), the user is not immediately revoked again because of inactivity or too many failed logons.

If the USER RESUME and USER SCHEDULE subcommands are used in a single USER command, the SCHEDULE subcommand is executed *before* the RESUME subcommand.

The RESUME subcommand has no parameters; it has the following syntax:

```
RESUME
```

SCHEDULE: The SCHEDULE subcommand can be used to maintain revoke and resume *schedules*, for example, to set up and maintain the periods of time during which the user is able to logon. The concept of revoke/revoke schedules is explained in Revoke/resume schedules.

The SCHEDULE subcommand is used to add or delete scheduled revoke and resume actions; this can cause the target user's revoke and resume dates to be changed, and can cause the user to become revoked or resumed.

The SCHEDULE subcommand has the following syntax:

```
SCHEDULE schedule action date [ reason ]
schedule    Name of the schedule; see below.
action      Any SCHEDULE action; see below.
date        Date or period for the SCHEDULE action; see below.
reason      Optional reason for the schedule action; see below.
```

If the USER RESUME and USER SCHEDULE subcommands are used in a single USER command, the SCHEDULE subcommand is executed before the RESUME subcommand.

Schedule *names* are words of up to 8 alphanumerical characters; names are not case-sensitive. The names can be determined by the installation as they see fit, e.g. 'REVOKE' for a schedule limited to system administrators, and 'DECENTRL' for a schedule that decentral administrators use. Access to schedules is restricted using *schedule* profiles, see Schedule profiles. Different schedule names have no priority over each other. Decentral administrators that have different scopes can safely be granted access to the same schedule names: each decentral administrator is able to apply the schedule only within his own scope.

The SCHEDULE actions are:

Table 612. Actions for CKGRACF USER SCHEDULE

Action	Meaning
ENABLE	Enable (for example, resume) the user from the date specified or for the period specified. A user will only be resumed if all schedules agree. If a period is specified, the user will be revoked after the period ends.
DISABLE	Disable (for example, revoke) the user from the date specified or for the period specified. A user will be revoked if revoked on *any* schedule. If a period is specified, the user will be resumed after the period ends, unless another schedule determines the user should be revoked.

Table 612. Actions for CKGRACF USER SCHEDULE (continued)

Action	Meaning
WIPE	Delete the action from the schedule, either one action if one date is specified or all actions for a period if a range is specified.

If an action changes the overall effect of the schedules, the user's revoke status and revoke and resume dates are changed.

With the SCHEDULE subcommand and the ENABLE or DISABLE action, either a single date or a single period can be specified in the following manner:

Table 613. Date formats for CKGRACF USER SCHEDULE

Option	Meaning
START-DATE	Enable or disable the user from the date specified. The effect of the action is indefinite. All actions scheduled for START-DATE and later dates within the schedule are wiped. For example, `SCHEDULE HARD DISABLE TODAY` would revoke the user as of today.
(START-DATE:END-DATE)	Perform the action from the start-date to the end-date. Both dates are included in the period. For example, `ENABLE(01OCT1998:01NOV1998)` enables from Oct 1 up to and *including* Nov 1). Any previously scheduled actions covering this period are wiped, scheduled actions outside of this period are not affected.
(START-DATE,LENGTH)	Perform the action from the start-date for the number of days specified by LENGTH. For example, `ENABLE (01OCT1998,2)` enables the user from Oct 1 up to and including Oct 2, but not including Oct 3. The length must be in the range 1 to 500. Any previously scheduled actions covering this period are wiped, scheduled actions outside of this period are not affected.

Notes:

1. The parentheses are not required.
2. With a REQUEST or ASK, the start-date must be today or a future date.
3. A date has the format `01OCT1998` or (Julian date) `1998/274` , or the literal value TODAY.
4. Wiped schedules remain in the profile as part of the audit trail for an additional period. Only after the audit period has passed they will be physically wiped from the profile.

With the SCHEDULE subcommand and the WIPE action, either a single date or a single period can be specified in the following manner:

Table 614. Date formats for CKGRACF USER SCHEDULE WIPE

Option	Meaning
START-DATE	For the schedule indicated, wipe the action set for that date.
(START-DATE:END-DATE)	For the schedule indicated, wipe all actions for the period specified. The start and end dates are included in the period. For example, the command `WIPE (01OCT1998:01NOV1998)` wipes scheduled actions from Oct 1 up to and *including* Nov 1.

Table 614. Date formats for CKGRACF USER SCHEDULE WIPE (continued)

Option	Meaning
(START-DATE,LENGTH)	For the schedule indicated, wipe all actions from the start-date for the number of days specified by LENGTH. For example, the command `WIPE (01OCT1998,2)` wipes scheduled actions from Oct 1 up to and including Oct 2, but not including Oct 3. The length must be in the range 1 to 500.

See Revoke/resume schedules for an explanation and examples of schedules.

REASON: The optional *reason* string is stored with the scheduled revoke/resume settings or with the command as a whole when there is no SCHEDULE subcommand defined. The string is used to add an explanation or reason for the action.

It is specified in the following manner:

```
REASON(reason)
reason      A reason string (See also Reason keywords in CKGRACF)
```

If the target userid is subject to multiple-authority, the reason specified with the REQUEST action is used; for later actions, any reason specified is ignored.

Note: If a non-restructured database is used and the command is queued because the target userid is subject to multiple-authority, the reason string might not fit into the USR entry used to store the queued command. In that case, the reason is truncated and message CKG627I is issued.

Revoke/resume schedules

CKGRACF provides a revoke and resume schedule facility that permits different decentralized administrators to set several future revoked or resumed periods. This function is supported for de-centralized administrators that do not have the group-SPECIAL attribute over the affected user profiles. The revoke and resume schedule process works in the following way:

- The installation can define any number of schedules. A schedule is identified by a name of 1 to 8 alphanumerical characters. Update of a schedule is granted through the name of the schedule.
- Each schedule consists of a list of dates, with one action per date. An action can be ENABLE or DISABLE. Within any single schedule, the effect of the schedule on the user depends on the last action only; two DISABLEs followed by a single ENABLE leads to an enabled user.
- All users have their own scheduled actions, and all schedules are independent. The COURSES schedule for PETER does not affect the COURSES schedule for ROB; the VACATIONS schedule for PETER does not affect the COURSES schedule for PETER.
- If multiple schedules are set for a single user–that is, the userid has scheduled actions for more than one schedule name–, the user will be revoked if disabled by *any* schedule. A *hard* revoke can be implemented by creating the schedule REVOKE, granting access to the system administrator only, and then disabling a user on that schedule. Other schedules are not able to resume the user.
- System and decentralized administrators can have access to different schedules. To alter a schedule, the administrator must have: (a) access to the

CKGRACF USER SCHEDULE command; (b) access to the schedule; and (c) the target user must lie within the CKGRACF-defined scope.

- A userid is revoked if revoked by *any* schedule. The userid is only to be resumed if all schedules agree.
- Any schedule can be altered to *enable* the user from a date or for a period of time; the user will be resumed by this schedule until the end of the period, and be revoked afterwards. A schedule can also be altered to *disable* the user from a date or for a period of time; the user will be revoked for at least this period of time, and resumed afterwards, unless he is revoked by any other schedule. Finally, any scheduled setting or all settings during a period of time can be *wiped*. During the period of time for which the scheduled actions were wiped, the userid is subject to the overall result of unwiped previous actions combined with the other schedules.
- During the period of time before the first scheduled action applies, or if no scheduled actions have been set at all, the revoke status of the user is not determined by the schedules. As long as the scheduled actions do not determine the revoke status, the schedules do not override the ALTUSER REVOKE or ALTUSER RESUME command. After any scheduled action has been applied, the schedules determine the user's revoke status, and override the ALTUSER REVOKE or ALTUSER RESUME command.
- The CKGRACF LIST USER command (see "LIST" on page 1515) can be used to display the scheduled actions for a userid, as well as the overall revoke/resume schedule that is the result of combining all scheduled actions.
- The CKGRACF RESUME command will only resume the user if the user is not subject to scheduled actions, or if the scheduled actions for the user allow a resume.
- The CKGRACF REFRESH command should be used to evaluate the schedules of a user, and apply any actions due today. For more information see "REFRESH" on page 1527.

Example: simple definitions: Two group administrators must both be able to specify a holiday schedule for users within their separate groups. There is also a central administrator who is only allowed to administer the 'hard' revoke schedule.

The schedule names defined are HOLIDAY and REVOKE; we assume the scope of the decentral administrators has already been defined. The administrators also need UPDATE access to the USER SCHEDULE command.

```
rdefine xfacilit ckg.schedule.holiday uacc(none)
permit ckg.schedule.holiday class(xfacilit) id(grp1adm grp2adm) +
access(update)
rdefine xfacilit ckg.schedule.revoke uacc(none)
permit ckg.schedule.revoke class(xfacilit) id(centradm) access(update)
```

Example revoke and resume schedules:

- "Creating a simple schedule" on page 1545
- "Revoking and resuming schedules before and after a the schedule applies" on page 1545
- "Using wiping actions" on page 1546
- "Revoking and resuming behavior based on multiple schedules" on page 1546
- "Implementing a hard revoke action" on page 1547
- "Setting up a schedule for selective system access over multiple periods" on page 1548

Creating a simple schedule: The following figure shows the revoke status of user PETER. In January, a single revoke period has been scheduled from August 1 to August 31. On March 1, PETER makes excessive logon attempts, which cause him to be revoked. On March 5, the CKGRACF USER RESUME command is used to resume the user, and the scheduled revoke period in August still applies.

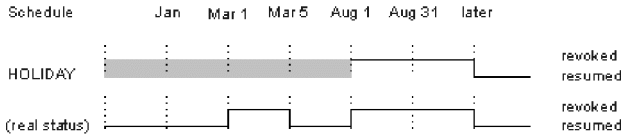


Figure 517. Simple revoke schedule

Note that, before August 1, the revoke status was not determined by the schedules; after August 31, the schedules do determine the revoke status.

The commands to achieve these schedules could have been:

```
CKGRACF USER PETER SCHEDULE HOLIDAY DISABLE (01AUG1998:31AUG1998)
--- excessive failed logons ---
CKGRACF USER PETER RESUME
```

Revoking and resuming schedules before and after a the schedule applies: To illustrate the effect of revoke and resume schedules for the period *before* the schedule first applies and the period after the schedule first applies, see the four figures below. In all cases, the schedules do not determine the revoke status before they first apply, but do determine the revoke status afterwards.

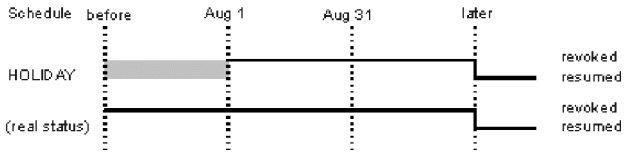


Figure 518. Revoked before schedule, a scheduled disabled period, and resumed afterwards

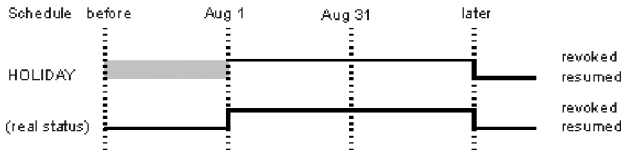


Figure 519. Resumed before schedule, a scheduled disabled period, and resumed afterwards

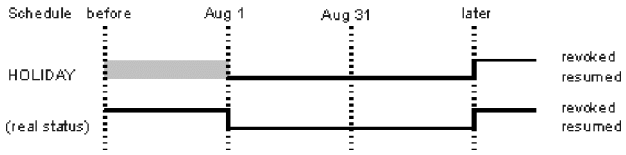


Figure 520. Revoked before schedule, a scheduled enabled period, and revoked afterwards

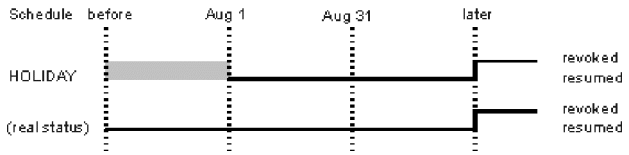


Figure 521. Resumed before schedule, a scheduled enabled period, and revoked afterwards

Using wiping actions: If a user is revoked or resumed due to scheduled actions, his status can be changed by adding another scheduled action. If the user should no longer be subject to a schedule (for example, the schedule HOLS98 is no longer used), the scheduled actions can also be wiped out. You can also use the wipe action if the scheduled actions were applied by mistake or for the wrong period (say, a year early).

If the wiped actions apply to future dates, the revoke status is not changed, and the revoke/resume date can be changed. If, however, the wiped actions apply to past dates or today, wiping the actions can change the user's current revoke status. The following cases can occur:

- After the actions have been wiped, the schedules still determine the user's current revoke status. In this case, message CKG121I or CKG122I is issued. These messages indicate whether the user's revoke status has changed after the wipe, and what the user's revoke status is set to as the result.
- After the actions have been wiped, the schedules do not determine the user's current revoke status. For instance, all scheduled actions were deleted, or all scheduled actions that have been left apply to future dates. In effect, this causes the user's revoke status *from the viewpoint of the schedules* to be undefined (the grey area in the preceding examples). Note that a RESUME command succeeds in resuming the user. In this case, message CKG122I or CKG123I is issued. Message CKG122I indicates that the user's revoke status has not changed after the wipe, and what the user's revoke status is set to. Message CKG123I indicates that the revoke status would have been left to revoked, but that the RESUME subcommand was also used. The user is resumed by the RESUME subcommand.
- You can use the WIPE command (see "WIPE" on page 1558) to remove all traces of a schedule from a profile.

Revoking and resuming behavior based on multiple schedules: This example illustrates revoke and resume behavior based on multiple schedules. This example is based on the following conditions:

- Two schedules have been created called COURSE and VACATION.
- On the VACATION schedule, the userid affected is revoked from January 15 to January 30; resumed on January 31, and revoked again from December 20 to January 1.
- On the COURSE schedule, the userid is revoked from May 1 to May 30 and is resumed on May 31.
-

Figure 522 on page 1547 shows a graph of the individual and combined schedules (overall).

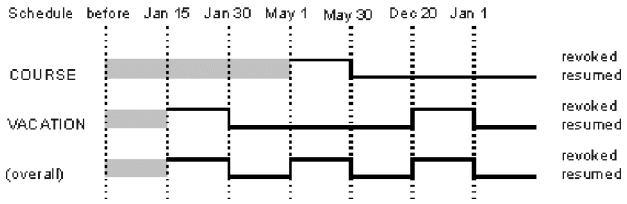


Figure 522. Multiple revoke/resume schedules

The following example shows the commands to create these schedules for userid *PETER*.

```
USER PETER SCHEDULE COURSE DISABLE (01MAY1998:30MAY1998)
USER PETER SCHEDULE VACATION DISABLE (15JAN1998:0JAN1998)
USER PETER SCHEDULE VACATION DISABLE (20DEC1998:01JAN1999)
```

You can use the following LIST command to list the scheduled actions for this user along with the resulting overall schedule: `CKGRACF LIST USER PETER`. See "LIST" on page 1515 for sample output of the LIST command.

Implementing a hard revoke action: This example describes the hard revoke action. The example is based on the following conditions:

- A userid for an external expert was disabled on schedule REVOKE from January 1.
- The same userid is enabled from August 1 for 7 days.
- The userid is finally revoked from August 8.

Based on these conditions, the userid revoke and resume status follows the REVOKE schedules shown in Figure 523.

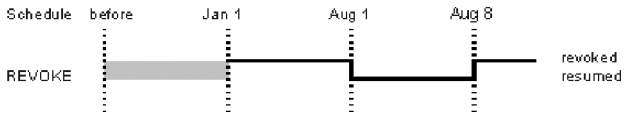


Figure 523. Hard revoke

The following example shows commands to create the REVOKE schedule for the userid *EXTERN*. In this example, the same schedule is used to revoke and resume the userid.

```
USER EXTERN SCHEDULE REVOKE DISABLE 01JAN1998
USER EXTERN SCHEDULE REVOKE ENABLE (01AUG1998,7)
```

If the userid had been configured to revoke on one schedule (REVOKE) and resumed on a different schedule (DECENTRL), the overall effect would have been as follows:

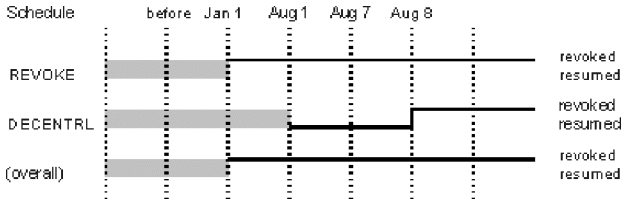


Figure 524. Multiple revokes

The resumed period of the DECENTRL schedule does not resume the user because the REVOKE schedule determines that the user should still be revoked.

The following example shows commands that could have been used to create the separate revoke and resume schedules.

```
USER EXTERN SCHEDULE REVOKE DISABLE 01JAN1998
USER EXTERN SCHEDULE DECENTRL ENABLE (01AUG1998,7)
```

Setting up a schedule for selective system access over multiple periods: This example describes selective system access. The scenario for this example is based on the following conditions:

- A userid for an external expert is created with status revoked.
- The external expert is to work on two projects, DB2 and CICS, and receives the following schedule for permits to the required data sets:
  - Enabled for DB2 and CICS from January 1 to May 1.
  - Enabled for CICS from August 1 to August 7
  - Enabled from August 10 to August 15.

Based on these conditions, the userid revoke and resume status follows the schedule shown in Figure 525, which will probably lead to an unexpected result.

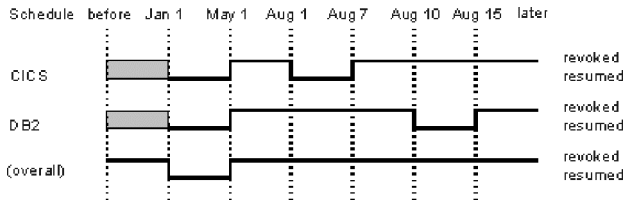


Figure 525. Multiple enabled periods

The reason for the unexpected result is that, if a user is enabled for a period, he is revoked afterwards. In this case, the resumed periods in August do not overlap, so the user remains revoked. The rationale is that the external expert should not be able to use his permits on DB2 data sets a week early.

If the user really needed to be resumed on both projects in August, the CICS and DB2 administrators need to work together.

- If the CICS project is over, the scheduled actions for the CICS profile should be wiped.
- If the user should be enabled for both projects, both administrators should agree, and both should enable him.
- If the user is going to work on one project one week, and another project another week, perhaps two different userids are required.

For the problem described in preceding paragraphs, revoke or resume schedules are not the solution. In this case, you should use temporary permits or connects.

Setting up multiple authority

CKGRACF provides for *multiple authority* to aid in the separation of powers. If a profile is subject to multiple-authority controls, any CKGRACF USER or CKGRACF CMD command for that profile must be validated by either one or two

other users before it is executed. This makes it possible to protect sensitive profiles from unauthorized alteration. The CKGRACF multiple-authority system functions in the following manner:

- Any profile can have a multiple-authority requirement, which is stored in the profile's USR field. If no requirement is stored in the profile, the installation-defined system-wide default is used. Setting a system-wide default enables the installation to define a multiple-authority requirement for all profiles that do not, or can not have a multiple-authority requirement set on them; This also defines the default multiple-authority requirement for all new profiles.
- The multiple-authority requirement affects the operation of the USER and CMD commands. Other commands are not subject to multiple-authority.
- The multiple-authority requirement for a profile is either SINGLE, DUAL or TRIPLE.
- There are two different actions you can use to initialize a command; The ASK and REQUEST actions. The ASK action is basically the same as the REQUEST action, with the exception that a REQUESTed command can be executed at once if the target profile has a SINGLE multiple-authority requirement, whereas an ASKed command will always be queued for later approval. This effectively entails that an ASKed command on a SINGLE multiple-authority profile will go through the same steps as a REQUESTed command for a DUAL multiple-authority profile.
- The multiple-authority requirement is either SINGLE, DUAL, or TRIPLE. Commands for single-authority profiles only need to be ratified or reviewed by one person with the authority to approve a command. Commands for dual-authority profiles need to be ratified or reviewed by two users with authority, while commands for triple-authority profiles need to be ratified or reviewed by three different users with authority. [23]
- A single profile's multiple authority requirement is set using the AUTHORITY command (see “AUTHORITY” on page 1503). Any profile without a multiple-authority requirement is subject to the default, which can be listed using the `SHOW CKRSITE` command (see “SHOW” on page 1529).
- If a command is issued for a profile which requires multiple-authority (for example, the requirement is not SINGLE) or the action is ASK, the command is *queued*. A queue of commands is stored in the profile's USR field. Subsequent CKGRACF commands can be issued to ratify or deny a queued command, as explained in the following text. Queued commands *expire* after an installation-defined period, or when they are not completed at the time they should have been executed (if AT is defined on the CMD command); expired commands can no longer be executed. After a command is completed (e.g. denied, executed, or expired), it is kept in the user profile until an *auditing period* has passed; after that period has expired, the command is deleted from the queue. All queued commands can be listed using the CKGRACF LIST command. The expiration period and auditing period can be listed using the SHOW CKRSITE command.
- Queued commands pass various *stages*, depending on the target profile's multiple-authority requirement. Commands for a dual-authority profile are requested, then completed; commands for a triple-authority profile are requested, seconded, and then completed. In each stage, actions must be performed by a userid different from the previous stages. The next section describes the possible actions and their effects.

23. A *user with authority* is defined as someone that can either REQUEST, SECOND or COMPLETE a command. The ASK command option is not considered an authoritative action.

- Authorization for each queued-command stage is granted separately. A help desk would have access to the REQUEST action, which executes commands for normal, single-authority userids, and queue commands for all other userids. The queued commands would then have to be ratified, and the help desk would not have authority to do this.
- If a group of administrators had access to both the REQUEST and COMPLETE actions, any administrator could request a command, and a colleague would have to ratify the command before it could be executed. This way you can implement a dual-sign administration policy. Another example would be an auditor who has access to the ASK action, not being able to actually execute anything, but able to request an approval, even for SINGLE multiple-authority profiles.

Actions on queued commands

A queued command must be acted on by entering the identical command again with a different queued-command action. Note that the easiest way to perform these actions is to use the Security zSecure ISPF interface to CKGRACF.

Table 615 lists the actions that can be performed on a queued command and describes the effect of the action.

Table 615. Actions on queued commands

Action	Effect
APPROVE	The command is approved and is either executed or passed to another person in order to be okayed.
HOLD	A decision is not made yet; expiration of the command is delayed. (Expiration counts from the last action. By repeatedly HOLDing a command, expiration can be delayed for a long time.)
DENY	The command is denied and can no longer be executed.
WITHDRAW	The command is withdrawn and can no longer be executed.

These actions are subject to the following rules:

- A command can only be approved, held, denied, or withdrawn if it still could be completed. After a command has been expired, denied, withdrawn, or executed, no further actions are possible.
- The WITHDRAW action can be performed by anyone with the authority to request the command. It is intended for use by the requesting user, in case a mistake has been made. A WITHDRAW action is allowed at any time until the command has been completed. After the command has been completed, a request must be made for the opposite action to 'undo' the command.
- The HOLD, DENY, or APPROVE actions must be used with SECOND or COMPLETE on queued commands. A command for a triple-authority userid passes from the SECOND to the COMPLETE stage by a SECOND APPROVE command. After the command has moved to the next stage, the seconding user can no longer deny the command.
- An action can only be performed by a user who was not involved in an earlier stage. This means that a requesting user is not able to second or complete a command (WITHDRAW is allowed). Similarly, a user who seconds a command cannot complete it. It *is* allowed to HOLD a command and then APPROVE or DENY it. Also, if a user SECOND HOLDs a command, and the command is then SECOND APPROVED by another user, the user who performed the HOLD can still complete the command.

The following tables list the actions initiated by REQ and the actions on a queued command initiated by ASK.

Table 616. Actions for queued command initiated with REQ

Previous action	Action	Authority	Effect
REQUEST	WITHDRAW	ALL	Withdrawn and not executed.
REQUEST	SECOND DENY	TRIPLE	Denied and not executed.
REQUEST	SECOND HOLD	TRIPLE	Held; expiration delayed.
REQUEST	SECOND APPROVE	TRIPLE	Approved; completion has to follow.
REQUEST	COMPLETE DENY	DUAL	Denied and not executed.
REQUEST	COMPLETE HOLD	DUAL	Held; expiration delayed.
REQUEST	COMPLETE APPROVE	DUAL	Approved and executed.
SECOND HOLD	WITHDRAW	ALL	Withdrawn and not executed.
SECOND HOLD	SECOND DENY	TRIPLE	Denied and not executed.
SECOND HOLD	SECOND HOLD	TRIPLE	Held; expiration delayed.
SECOND HOLD	SECOND APPROVE	TRIPLE	Approved; completion has to follow.
SECOND HOLD	COMPLETE DENY	DUAL	Denied and not executed.
SECOND HOLD	COMPLETE HOLD	DUAL	Held; expiration delayed.
SECOND HOLD	COMPLETE APPROVE	DUAL	Approved and executed.
SECOND APPROVE	WITHDRAW	TRIPLE	Withdrawn and not executed.
SECOND APPROVE	SECOND DENY	*error*	Issue not allowed error.
SECOND APPROVE	SECOND HOLD	*error*	Issue not allowed error.
SECOND APPROVE	SECOND APPROVE	*error*	Issue not allowed error.
SECOND APPROVE	COMPLETE DENY	TRIPLE	Denied and not executed.
SECOND APPROVE	COMPLETE HOLD	TRIPLE	Held; expiration delayed.
SECOND APPROVE	COMPLETE APPROVE	TRIPLE	Approved and executed.
COMPLETE HOLD	WITHDRAW	ALL	Withdraw and not executed.
COMPLETE HOLD	SECOND DENY	*error*	Issue not allowed error.
COMPLETE HOLD	SECOND HOLD	*error*	Issue not allowed error.
COMPLETE HOLD	SECOND APPROVE	*error*	Issue not allowed error.
COMPLETE HOLD	COMPLETE DENY	ALL	Denied and not executed.
COMPLETE HOLD	COMPLETE HOLD	ALL	Held; expiration delayed.
COMPLETE HOLD	COMPLETE APPROVE	ALL	Approved and executed.

Table 617. Actions for queued command initiated by ASK

Previous action	Action	Authority	Effect
ASK	WITHDRAW	ALL	Withdrawn and not executed.
ASK	SECOND DENY	DUAL/TRIPLE	Denied and not executed.
ASK	SECOND HOLD	DUAL/TRIPLE	Held; expiration delayed.
ASK	SECOND APPROVE	DUAL/TRIPLE	Approved; completion has to follow.
ASK	COMPLETE DENY	SINGLE	Denied and not executed.
ASK	COMPLETE HOLD	SINGLE	Held; expiration delayed.
ASK	COMPLETE APPROVE	SINGLE	Approved and executed.
SECOND HOLD	WITHDRAW	ALL	Withdrawn and not executed.
SECOND HOLD	SECOND DENY	DUAL/TRIPLE	Denied and not executed.
SECOND HOLD	SECOND HOLD	DUAL/TRIPLE	Held; expiration delayed.
SECOND HOLD	SECOND APPROVE	DUAL/TRIPLE	Approved; completion has to follow.
SECOND HOLD	COMPLETE DENY	SINGLE	Denied and not executed.
SECOND HOLD	COMPLETE HOLD	SINGLE	Held; expiration delayed.
SECOND HOLD	COMPLETE APPROVE	SINGLE	Approved and executed.
SECOND APPROVE	WITHDRAW	ALL	Withdrawn and not executed.
SECOND APPROVE	SECOND DENY	*error*	Issue not allowed error.
SECOND APPROVE	SECOND HOLD	*error*	Issue not allowed error.
SECOND APPROVE	SECOND APPROVE	*error*	Issue not allowed error.
SECOND APPROVE	COMPLETE DENY	DUAL/TRIPLE	Denied and not executed.
SECOND APPROVE	COMPLETE HOLD	DUAL/TRIPLE	Held; expiration delayed.
SECOND APPROVE	COMPLETE APPROVE	DUAL/TRIPLE	Approved and executed.
COMPLETE HOLD	WITHDRAW	ALL	Withdraw and not executed.
COMPLETE HOLD	SECOND DENY	*error*	Issue not allowed error.
COMPLETE HOLD	SECOND HOLD	*error*	Issue not allowed error.
COMPLETE HOLD	SECOND APPROVE	*error*	Issue not allowed error.
COMPLETE HOLD	COMPLETE DENY	ALL	Denied and not executed.
COMPLETE HOLD	COMPLETE HOLD	ALL	Held; expiration delayed.
COMPLETE HOLD	COMPLETE APPROVE	ALL	Approved and executed.

ASK is not allowed for TRIPLE authority profiles.

Creating random passwords

The PWSET RANDOM option creates a random encrypted password to be stored in the user profile. If the password encryption exit (ICHDEX01 or ICHDEX11) is set to DES-only, this option makes it practically impossible to logon for the userid. Note, however, that there is *no absolute guarantee* that logon is impossible. The description of the password check that follows explains how the passwords created by the PWSET RANDOM option are secured:

- When DES-encryption is used and a password is set, the encrypted password is calculated by DES-encrypting the userid with a key computed from the unencrypted password. The encrypted password is then stored.
- When a password is entered to be verified, the entered password is encrypted in the same way, and the encrypted passwords are compared. The encrypted passwords must be equal to match.
- A DES-encrypted password cannot be decrypted. The encryption is also unique, in the sense that there is no other password that has the same encrypted result.
- There is no easy way to guess a DES-encrypted password. The only way to do this is to try *all* possible passwords, encrypting them, and comparing the encrypted passwords. If a guess is almost correct, in the sense that it differs from the password in a very small way, the encrypted passwords are likely to be completely different.
- If two userids have the same password, the encrypted passwords are completely different. (The userid is used in the DES-encryption). Similarly, when two encrypted passwords are identical, the unencrypted passwords are completely different.

When a random value is used as an encrypted password, there is no way to check how 'hard' it is. There is exactly one password that results in the encrypted value, but which password it is depends both on the userid and the random value. It is almost certain that the unencrypted password cannot be found, and that it cannot be entered from a keyboard even if it was found, but there is a remote possibility that it will be easy (SECRET, for example').

Warning about passwords

RACF commands issued through CMD or USER PWSET can be logged in SMF–depending on the audit level of the CKG.CMD.CMD profile–and written to the job output if CKGRACF is run in batch. These commands can show passwords and password phrases.

When a PASSWORD or PHRASE parameter is recognized in a RACF command, the secret value is replaced by a question mark. To prevent password collection from the SMF or the job log, make sure that the PASSWORD or PHRASE parameter is not abbreviated to fewer than 4 positions and that the left parenthesis is coded immediately following the parameter with no spaces. The following examples shows the logging for different formats:

`ALTUSER IBMUSER PASS(1234)` is logged as `ALTUSER IBMUSER PASS(?)` with no password displayed.

`ALTUSER IBMUSER PAS(1234)` is logged as-is to SMF, displaying the password.

`ALTUSER IBMUSER PASSWORD (1234)` includes a blank before the opening parenthesis and is logged as-is, displaying the password.

`ALTUSER IBMUSER PHRASE (1234)` includes a blank before the opening parenthesis and is logged as-is, displaying the password.

Protecting a userid with the PWSET NOPASSWORD option

The PWSET NOPASSWORD option changes the status of the userid to protected. Protected userids cannot be used to enter the system by any means that would normally require a password or password phrase to be specified, such as TSO logon, CICS signon, or typical batch job submission. Therefore, userids that you assign to z/OS UNIX, UNIX daemons, started procedures, applications, servers or subsystems can be protected from being revoked when an incorrect password or password phrase is entered. If the user attempts to enter the system with a password or password phrase, the attempt fails.

The status of the userid is set to unprotected with a USER PWRESET command or with a USER PWSET command which is not followed by the NOPASSWORD option.

USRDATA

The USRDATA command can be used to set, delete, or list entries in a profile's USR field. This field can consist of multiple entries, each containing an *index* (value of USRNM field) and *data* (contents, the value of USRDATA field optionally followed by the value of USRFLG field). The contents and index names are completely at the site's discretion; a common example is PHONE. The USRDATA command works on the USRDATA (and USRFLG) field, using the value of the USRNM field as an index. A restriction on the USRDATA command is that index names starting with CNG are reserved for use by CKGRACF; the USRDATA command cannot be used to alter or list these USR entries. Index names starting with $C4R are reserved for zSecure Command Verifier. zSecure Command Verifier maintains these USR entries, so you should not directly update them. We recommend that you establish profiles that cover resources CKG.USRDATA.*.*.$C4R*, with UACC(NONE), and ACCESS(READ) for the RACF administrators and auditors.

Also, discrete data set profiles are not supported.

The USRDATA command has the following syntax:

```
USRDATA class profile ADD     [ REASON(reason) ] index(data) ...
USRDATA class profile DELETE  [ REASON(reason) ] index ...
USRDATA class profile DELETE  [ REASON(reason) ] index(data) ...
USRDATA class profile LIST    [ REASON(reason) ] index ...
USRDATA class profile REPLACE [ REASON(reason) ] index(old-data,new-data) ...
USRDATA class profile SET     [ REASON(reason) ] index(data) ...
```

```
class             Any valid RACF class
profile           Any valid RACF profile
action            One of ADD, DELETE, LIST, REPLACE, or SET; see below
index             The index (USRNM value) for the USR entry, with optional
index(data)       values for the USRDATA/USRFLG field; see below
index(old-data,new-data)
reason            A reason string (Reason keywords in CKGRACF)
```

The profile can be specified with profile conversion characters (See also “Profile conversion in CKGRACF” on page 1500).

If no conversion character `D` or `G` has been specified, the effect depends on the profile type. Data set profiles are treated as generics, since discrete data set profiles are not supported. This implies that fully qualified generics need not be quoted. General resource profiles are treated 'as-is': they are treated as a generic if the

name contains generic characters, and as a discrete if it does not. Since fully qualified generics are not allowed for general resource profiles, quotes should never be necessary.

Note:

> For DATASET profiles, the full name must be specified. Unquoted data set profiles are *not* prefixed with the user's TSO prefix.

Each *data* value is a USRDATA value optionally followed by a slash (/) and a USRFLAG value. A USRDATA value must be specified as a string with a maximum size of 255 characters (quotes and conversions are allowed). An USRFLG value is a number between 0 and 255 which can be written in decimal form (e.g. 160) or hexadecimal form (e.g. 'A0'X). If an USRFLG value is to be specified, quotes around the preceding USRDATA value are obligatory. Without the quotes, the slash and the (decimal) value following it will be treated as part of the USRDATA value. The *action* determines whether a USRDATA (and USRFLG) value can or must be specified, as described in the following table.

Table 618. Actions for CKGRACF USRDATA

Action	Values	Effect	Example
ADD	one	Adds an USR entry with USRNM value *index* and USRDATA/USRFLG value *data*.	ADD *index(data)*
DELETE	none	Deletes all USR entries with USRNM value*index*.	DELETE *index*
DELETE	one	Deletes all USRDATA entries with USRNM value *index* and USRDATA/USRFLG value *data*.	DELETE *index(data)*
LIST	none	Lists the USRDATA field of all USR entries with USRNM value *index*. Note: an exact value must be specified, patterns are not allowed.	LIST *index*
REPLACE	two	If any USR entries can be found with USRNM value *index* and USRDATA/USRFLG value *old-data*, these are deleted and replaced by a single entry with USRNM value *index* and USRDATA/USRFLG value *new-data*.	REPLACE *index(old-data,new-data)*
SET	one	Deletes any USR entries with USRNM value *index*, if present; then adds a single USR entry with USRNM value *index* and USRDATA/USRFLG value *data*.	SET *index(data)*

More than one index can be specified in a single USRDATA command; the same action is applied to each of the indices and values in turn. The target profile is not changed if an error occurs within a single USRDATA command.

When the USRFLG value of an entry is not zero, the USRDATA LIST command will print it as a hexadecimal number after a slash after the corresponding, quoted, USRDATA value. When the USRFLG value is zero, the slash and hexadecimal number is not printed.

If the USRFLAG value is left away in ADD *index(data)*, or SET *index(data)*, or in the *new-data* of REPLACE *index(old-data, new-data)*, the USRFLG value will be 0 by default. If the USRFLG value is left away in DELETE*index(data)*, entries with USRNM value *index*, USRDATA value *data*, and any USRFLG value will be deleted. If the USRFLG value is left away in *old-data* of REPLACE *index(old-data, new-data)*, entries with USRNM value *index*, USRDATA value *old-data*, and any USRFLG value will be deleted before replacing them with *index(new-data)*.

The USRDATA command requires access to the command profile shown in the following table.

Table 619. Command access checks for CKGRACF USRDATA

Resource name checked	Access required
CKG.CMD.USRDATA	READ for the LIST option; UPDATE for all other options.

In addition, the target user must be within the userdata-scope of the command user (see "CKGRACF authority checks" on page 1559):

Table 620. USRDATA access checks for CKGRACF USRDATA

Resource name checked	Access required
CKG.USRDATA.OWN.*class.index*	READ for the LIST option; UPDATE for all other options.
CKG.USRDATA.ALL.*class.index*	READ for the LIST option; UPDATE for all other options.
CKG.USRDATA.SCP.*class.index*	READ for the LIST option; UPDATE for all other options.

If access to CKG.USRDATA.SCP.*class.index* is defined, the following profiles will be checked:

Table 621. Scope access checks for CKGRACF USRDATA

Resource name checked	Access required
CKG.SCP.ID.*userid.owner.dfltgrp*	READ for the LIST option; UPDATE for all other options.
CKG.SCP.ID.*groupid.owner*	READ for the LIST option; UPDATE for all other options.
CKG.SCP.G.*groups...*	READ for the LIST option; UPDATE for all other options.
CKG.SCP.U.*user.groups...*	READ for the LIST option; UPDATE for all other options.

Restrictions

There are several restrictions on the use of the USR field and the USRDATA command:

- The USRDATA command does not support discrete data set profiles. The reason is that most DASD management packages (including DMS and HSM) do not preserve the USR field on their backups of discrete profiles. This does not apply to generic profiles, so it is feasible to store e.g. data set account numbers in the generic data set profiles.

- The USRDATA command should not be used to store information that needs to be checked from RACF exits. This is because RACF does not read the info by itself and also does not cache it with the ACEE. Hence using the USR field from an exit might severely impact performance. Use an installation-defined RACLISTed profile class instead.
- The Security zSecure RECREATE command does not recreate the full USR field. It recreates the multiple-authority setting and installation-defined entries.
- The Security zSecure COPY command does not copy USR fields.

Example

In this example, we assume that index DB2PROJ indicates a DB2 project name. The central administrators set this value for each group using DB2, decentral administrators can list this value for groups within their scope.

We assume the following example profiles:

Table 622. Example profiles for CKGRACF USRDATA

Profile name	Central	Decentral	Comment
CKG.CMD.USRDATA	UPDATE	READ or UPDATE	Grant decentral administrators READ access if they cannot update any USR field; grant UPDATE if they may update some USR fields.
CKG.USRDATA.ALL.GROUP.DB2PROJ	UPDATE	NONE	Central administrators list and update DB2PROJ for all groups.
CKG.USRDATA.SCP.GROUP.DB2PROJ	NONE	READ	Decentral administrators list DB2PROJ for groups within their scope.
CKG.SCP.ID.*db2grp.db2ownr*.*	NONE	READ or UPDATE	Group scope for decentral administrators.
CKG.SCP.G.***.db2group...*	NONE	READ or UPDATE	Group scope for decentral administrators.

In this setup, a central administrator could set DB2PROJ for group DB2DEV using the command:

```
ckgracf usrdata group db2dev set db2proj('Developers')
```

A decentral administrator with group DB2DEV within his scope could display this value using the command:

```
ckgracf usrdata group db2dev list db2proj
```

WIPE

The WIPE command can be used to delete part of the USRDATA from user group, dataset, and general resource profiles, including the CKGRACF settings. The CKGRACF settings are stored in the profile's USR field, but cannot be altered by the USRDATA command. Use the LIST command (with the QUEUE or TAG option) to display these settings.

The WIPE command has the following syntax:

```
WIPE class profile action ... [ REASON(reason) ]

class     Any valid RACF class.
profile   Any valid RACF profile.
action    A WIPE action; one or more actions may be specified
reason    A reason string ("Reason keywords in CKGRACF" on page 1501)
```

The WIPE actions are specified in the following table.

Table 623. Actions for CKGRACF WIPE

Action	Meaning
ALL	Wipe all userdata entries
AUTHORITY	Wipe authority settings (same effect as AUTHORITY DEFAULT)
DEFAULTPW	Wipe the default password (same effect as USER PWDEFAULT DELETE)
INSTALLATION	Wipe all installation-defined USR entries (that is, all entries that are not reserved for use by CKGRACF)
QUEUE	Wipe all queued commands
RESERVED	Wipe all CKGRACF-reserved entries
SCHEDULE	Wipe the scheduled revoke/resume settings
UNDEFINED	Wipe all CKGRACF-reserved, undefined entries

For each option used, access is required to the command resource name shown in the following table.

Table 624. Command access checks for CKGRACF WIPE

Option	Resource name checked	Access required
ALL	CKG.CMD.WIPE.ALL	UPDATE
AUTHORITY	CKG.CMD.WIPE.AUTHORITY	UPDATE
DEFAULTPW	CKG.CMD.WIPE.DEFAULTPW	UPDATE
INSTALLATION	CKG.CMD.WIPE.INSTALLATION	UPDATE
QUEUE	CKG.CMD.WIPE.QUEUE	UPDATE
RESERVED	CKG.CMD.WIPE.RESERVED	UPDATE
SCHEDULE	CKG.CMD.WIPE.SCHEDULE	UPDATE
UNDEFINED	CKG.CMD.WIPE.UNDEFINED	UPDATE

The WIPE command is not subject to scope checks.

Note that WIPE SCHEDULE deletes *all* scheduled actions, and the schedule audit trail, from a profile. The USER SCHEDULE WIPE command wipes selected scheduled actions from a single schedule, and keeps an audit trail.

Example

In order to wipe *all* USR entries from the user profile IBMUSER, use CKGRACF WIPE USER IBMUSER ALL. In order to wipe all CKGRACF-defined entries (and leave all installation-defined entries), use CKGRACF WIPE USER IBMUSER RESERVED.

The CARLa script CKGXUSRW generates CKGRACF WIPE and USRDATA commands to delete USR entries. A command is generated for each type of entry; this allows you to keep those entries that you do not want to delete.

This CARLa script can be used with job C2RJXRFR in the SCKRSAMP library by specifying it as the MEMBER:

```
//CKRCARLA EXEC C2RC,MEMBER=CKGXUSRW,OPTCARLA=,ALLOCUNL=1,
//         CONFIG=C2R$PARM
```

CKGRACF authority checks

CKGRACF performs its own authority checks and logging through normal RACF requests. Authority to operate on user, group, general resource and data set profiles is regulated through CKGRACF scope profiles. Authority to the specific CKGRACF commands and options is regulated through CKGRACF command profiles. The authority to operate on individual fields is regulated through racfdata profiles. Authority to specific site-defined *schedules* and *userdata fields* is regulated through CKGRACF schedule profiles and userdata profiles.

The capabilities provided through CKGRACF are an addition to the standard RACF authority a user has; they do not reduce a user's authority unless you also take the standard RACF authority away (for example, replace standard RACF functionality by CKGRACF functionality).

The CKGRACF profiles reside in the XFACILIT class or another, installation-defined, class.

All these RACF profile types are explained in the following sections.

Command profiles

Access to the CKGRACF commands is determined using command profiles; these profiles start with CKG.CMD. CKGRACF checks a resource name of the form CKG.CMD.*command.action.option*; the qualifiers are used where applicable.

The following table lists the various resource names that CKGRACF checks:

Table 625. Command access checks for all CKGRACF commands

Command and option	Resource name checked
ACCESS	CKG.CMD.ACCESS.ALL
AUTHORITY *class*	CKG.CMD.AUTHORITY.*class*
CMD ASK CONNECT	CKG.CMD.CMD.ASK.CONNECT
CMD ASK DELDSD	CKG.CMD.CMD.ASK.DELDSD
CMD ASK PERMIT	CKG.CMD.CMD.ASK.PERMIT
CMD ASK RDELETE	CKG.CMD.CMD.ASK.RDELETE
CMD ASK REMOVE	CKG.CMD.CMD.ASK.REMOVE
CMD COMPLETE CONNECT	CKG.CMD.CMD.CMP.CONNECT

Table 625. Command access checks for all CKGRACF commands (continued)

Command and option	Resource name checked
CMD COMPLETE DELDSD	CKG.CMD.CMD.CMP.DELDSD
CMD COMPLETE PERMIT	CKG.CMD.CMD.CMP.PERMIT
CMD COMPLETE RDELETE	CKG.CMD.CMD.CMP.RDELETE
CMD COMPLETE REMOVE	CKG.CMD.CMD.CMP.REMOVE
CMD EXECUTE ADDGROUP	CKG.CMD.CMD.EX.ADDGROUP
CMD EXECUTE ADDSD	CKG.CMD.CMD.EX.ADDSD
CMD EXECUTE ADDUSER	CKG.CMD.CMD.EX.ADDUSER
CMD EXECUTE ALTDSD	CKG.CMD.CMD.EX.ALTDSD
CMD EXECUTE ALTGROUP	CKG.CMD.CMD.EX.ALTGROUP
CMD EXECUTE ALTUSER	CKG.CMD.CMD.EX.ALTUSER
CMD EXECUTE CONNECT	CKG.CMD.CMD.EX.CONNECT
CMD EXECUTE DEFINE	CKG.CMD.CMD.EX.DEFINE
CMD EXECUTE DELETE	CKG.CMD.CMD.EX.DELETE
CMD EXECUTE DELDSD	CKG.CMD.CMD.EX.DELDSD
CMD EXECUTE DELGROUP	CKG.CMD.CMD.EX.DELGROUP
CMD EXECUTE DELUSER	CKG.CMD.CMD.EX.DELUSER
CMD EXECUTE HELP	CKG.CMD.CMD.EX.HELP
CMD EXECUTE LISTGRP	CKG.CMD.CMD.EX.LISTGRP
CMD EXECUTE LISTDSD	CKG.CMD.CMD.EX.LISTDSD
CMD EXECUTE LISTUSER	CKG.CMD.CMD.EX.LISTUSER
CMD EXECUTE PASSWORD	CKG.CMD.CMD.EX.PASSWORD
CMD EXECUTE PERMIT	CKG.CMD.CMD.EX.PERMIT
CMD EXECUTE RACDCERT	CKG.CMD.CMD.EX.RACDCERT
CMD EXECUTE RACLINK	CKG.CMD.CMD.EX.RACLINK
CMD EXECUTE RACMAP	CKG.CMD.CMD.EX.RACMAP
CMD EXECUTE RALTER	CKG.CMD.CMD.EX.RALTER
CMD EXECUTE RDEFINE	CKG.CMD.CMD.EX.RDEFINE
CMD EXECUTE RDELETE	CKG.CMD.CMD.EX.RDELETE
CMD EXECUTE REMOVE	CKG.CMD.CMD.EX.REMOVE
CMD EXECUTE RLIST	CKG.CMD.CMD.EX.RLIST
CMD EXECUTE SEARCH	CKG.CMD.CMD.EX.SEARCH
CMD EXECUTE SETROPTS	CKG.CMD.CMD.EX.SETROPTS
CMD REQUEST CONNECT	CKG.CMD.CMD.REQ.CONNECT
CMD REQUEST DELDSD	CKG.CMD.CMD.REQ.DELDSD
CMD REQUEST PERMIT	CKG.CMD.CMD.REQ.PERMIT
CMD REQUEST RDELETE	CKG.CMD.CMD.REQ.RDELETE
CMD REQUEST REMOVE	CKG.CMD.CMD.REQ.REMOVE
CMD SECOND CONNECT	CKG.CMD.CMD.SEC.CONNECT
CMD SECOND DELDSD	CKG.CMD.CMD.SEC.DELDSD
CMD SECOND PERMIT	CKG.CMD.CMD.SEC.PERMIT

Table 625. Command access checks for all CKGRACF commands (continued)

Command and option	Resource name checked
CMD SECOND RDELETE	CKG.CMD.CMD.SEC.RDELETE
CMD SECOND REMOVE	CKG.CMD.CMD.SEC.REMOVE
CMD WITHDRAW CONNECT	CKG.CMD.CMD.REQ.CONNECT
CMD WITHDRAW DELDSD	CKG.CMD.CMD.REQ.DELDSD
CMD WITHDRAW PERMIT	CKG.CMD.CMD.REQ.PERMIT
CMD WITHDRAW RDELETE	CKG.CMD.CMD.REQ.RDELETE
CMD WITHDRAW REMOVE	CKG.CMD.CMD.REQ.REMOVE
CKGAUTH *class*	CKG.CMD.CKGAUTH.*class*
COMMENT	CKG.CMD.COMMENT
FIELD INTERVAL	CKG.CMD.FIELD.INTERVAL
FIELD LJDATE	CKG.CMD.FIELD.LJDATE
FIELD LJTIME	CKG.CMD.FIELD.LJTIME
FIELD PASSDATE	CKG.CMD.FIELD.PASSDATE
FIELD PASSWORD	CKG.CMD.FIELD.PASSWORD
FIELD PHRASE	CKG.CMD.FIELD.PHRASE
FIELD PHRDATE	CKG.CMD.FIELD.PHRDATE
FIELD REVOKECT	CKG.CMD.FIELD.REVOKECT
FIELD TCOMMAND	CKG.CMD.FIELD.TCOMMAND
FIELD TUPT	CKG.CMD.FIELD.TUPT
LIST	CKG.CMD.LIST
PWCONVERT	CKG.CMD.PWCONVERT
RDELETE	CKG.CMD.RDELETE
REFRESH	CKG.CMD.REFRESH
SHOW MYACCESS	CKG.CMD.SHOW.MYACCESS
SHOW MYACCESS ID *id*	CKG.CMD.SHOW.MYACCESS CKG.CMD.ACCESS.ALL
USER INTERVAL ASK	CKG.CMD.USER.ASK.INTERVAL
USER INTERVAL REQUEST	CKG.CMD.USER.REQ.INTERVAL
USER INTERVAL WITHDRAW	CKG.CMD.USER.REQ.INTERVAL
USER INTERVAL SECOND	CKG.CMD.USER.SEC.INTERVAL
USER INTERVAL COMPLETE	CKG.CMD.USER.CMP.INTERVAL
USER NOINTERVAL ASK	CKG.CMD.USER.ASK.NOINTERVAL
USER NOINTERVAL REQUEST	CKG.CMD.USER.REQ.NOINTERVAL
USER NOINTERVAL WITHDRAW	CKG.CMD.USER.REQ.NOINTERVAL
USER NOINTERVAL SECOND	CKG.CMD.USER.SEC.NOINTERVAL
USER NOINTERVAL COMPLETE	CKG.CMD.USER.CMP.NOINTERVAL
USER PWDEFAULT ASK	CKG.CMD.USER.ASK.PWDEFAULT
USER PWDEFAULT REQUEST	CKG.CMD.USER.REQ.PWDEFAULT
USER PWDEFAULT WITHDRAW	CKG.CMD.USER.REQ.PWDEFAULT
USER PWDEFAULT SECOND	CKG.CMD.USER.SEC.PWDEFAULT

Table 625. Command access checks for all CKGRACF commands (continued)

Command and option	Resource name checked
USER PWDEFAULT COMPLETE	CKG.CMD.USER.CMP.PWDEFAULT
USER PWNOEXIT ASK	CKG.CMD.USER.ASK.PWNOEXIT
USER PWNOEXIT REQUEST	CKG.CMD.USER.REQ.PWNOEXIT
USER PWNOEXIT WITHDRAW	CKG.CMD.USER.REQ.PWNOEXIT
USER PWNOEXIT SECOND	CKG.CMD.USER.SEC.PWNOEXIT
USER PWNOEXIT COMPLETE	CKG.CMD.USER.CMP.PWNOEXIT
USER PWNOHIST ASK	CKG.CMD.USER.ASK.PWNOHIST
USER PWNOHIST REQUEST	CKG.CMD.USER.REQ.PWNOHIST
USER PWNOHIST WITHDRAW	CKG.CMD.USER.REQ.PWNOHIST
USER PWNOHIST SECOND	CKG.CMD.USER.SEC.PWNOHIST
USER PWNOHIST COMPLETE	CKG.CMD.USER.CMP.PWNOHIST
USER PWNORULE ASK	CKG.CMD.USER.ASK.PWNORULE
USER PWNORULE REQUEST	CKG.CMD.USER.REQ.PWNORULE
USER PWNORULE WITHDRAW	CKG.CMD.USER.REQ.PWNORULE
USER PWNORULE SECOND	CKG.CMD.USER.SEC.PWNORULE
USER PWNORULE COMPLETE	CKG.CMD.USER.CMP.PWNORULE
USER PWRESET ASK	CKG.CMD.USER.ASK.PWRESET
USER PWRESET REQUEST	CKG.CMD.USER.REQ.PWRESET
USER PWRESET WITHDRAW	CKG.CMD.USER.REQ.PWRESET
USER PWRESET SECOND	CKG.CMD.USER.SEC.PWRESET
USER PWRESET COMPLETE	CKG.CMD.USER.CMP.PWRESET
USER PWSET ASK	see table Table 606 on page 1534
USER PWSET REQUEST	see table Table 606 on page 1534
USER PWSET SECOND	see table Table 606 on page 1534
USER PWSET COMPLETE	see table Table 606 on page 1534
USER RACLINK UNDEF ASK	CKG.CMD.USER.ASK.RACLINK.UNDEF
USER RACLINK UNDEF REQUEST	CKG.CMD.USER.REQ.RACLINK.UNDEF
USER RACLINK UNDEF WITHDRAW	CKG.CMD.USER.REQ.RACLINK.UNDEF
USER RACLINK UNDEF SECOND	CKG.CMD.USER.SEC.RACLINK.UNDEF
USER RACLINK UNDEF COMPLETE	CKG.CMD.USER.CMP.RACLINK.UNDEF
USER RESUME ASK	CKG.CMD.USER.ASK.RESUME
USER RESUME REQUEST	CKG.CMD.USER.REQ.RESUME
USER RESUME WITHDRAW	CKG.CMD.USER.REQ.RESUME
USER RESUME SECOND	CKG.CMD.USER.SEC.RESUME
USER RESUME COMPLETE	CKG.CMD.USER.CMP.RESUME
USER SCHEDULE ASK	CKG.CMD.USER.ASK.SCHEDULE
USER SCHEDULE REQUEST	CKG.CMD.USER.REQ.SCHEDULE
USER SCHEDULE WITHDRAW	CKG.CMD.USER.REQ.SCHEDULE
USER SCHEDULE SECOND	CKG.CMD.USER.SEC.SCHEDULE
USER SCHEDULE COMPLETE	CKG.CMD.USER.CMP.SCHEDULE

Table 625. Command access checks for all CKGRACF commands (continued)

Command and option	Resource name checked
USRDATA	CKG.CMD.USRDATA
WIPE ALL	CKG.CMD.WIPE.ALL
WIPE AUTHORITY	CKG.CMD.WIPE.AUTHORITY
WIPE DEFAULTPW	CKG.CMD.WIPE.DEFAULTPW
WIPE INSTALLATION	CKG.CMD.WIPE.INSTALLATION
WIPE QUEUE	CKG.CMD.WIPE.QUEUE
WIPE RESERVED	CKG.CMD.WIPE.RESERVED
WIPE SCHEDULE	CKG.CMD.WIPE.SCHEDULE
WIPE UNDEFINED	CKG.CMD.WIPE.UNDEFINED

The access required to these profiles is READ for operations that list information, and UPDATE for operations that can change information. The PWCONVERT and RDELETE commands also require that the user has the system-wide SPECIAL attribute. In the command language reference, the description of each command notes the access required to the command profiles.

Note that for the USER, LIST, and USRDATA commands, access to the command profile is not sufficient. The USER and LIST commands require that the target user is within the scope of the command user; this requires access to the correct scope profiles. The USER SCHEDULE command also requires access to the target schedule; this requires access to the schedule profiles; see below. The USRDATA command requires access to the userdata index; this requires access to the userdata profiles; see below. The CMD command can require access to the racfdata profiles; also see below.

Scope profiles

Scope profiles are used to define the users, groups and profiles that lie within the scope of a user. They can for example be used to define a scope for a decentral administrator to CKGRACF. This scope is rather different from the RACF-defined scope for a group administrator. The CKGRACF scope is based upon the ownership-tree of a resource. Access through CKGRACF is regulated by the access granted by two different checks: ID profile checks (CKG.SCP.ID), and user/group (U/G) profile checks (CKG.SCP.U or CKG.SCP.G). ID profiles permit access directly based on the groupid/userid associated with the target object. SCP.U/G profiles use the ownership tree of the target object, with as top qualifier either a user (for SCP.U profiles) or a group (for SCP.G profiles).

Note that for all occurrences of CKG.SCP a profile with the identical function exists specifically for the ASK command stage. This profile is CKG.SCPASK. A requested command will check the CKG.SCP profiles, while an asked command will check the CKG.SCPASK profiles.

Using RACF-defined scopes with CKGRACF

READ or higher access to the CKG.SCP.RACF resource extends a user's CKGRACF scope with the user's RACF-defined scope. The following specification of this CKGRACF scope extension uses the concept of a *group owner chain*. The group owner chain of a user or group *id* is the sequence *groupx*, ..., *group2*, *group1*, *id* where *groupx* is equal to SYS1 or the owner of *groupx* or *id* is an userid, and where

each *groupx*, ..., *group2*, *group1* is a group which is the owner of the resource which immediately follows it. Note that if *id* is a group, it is included with the group owner chain of *id*.

If *userid* requests *access* to *resource*, and *userid* has READ access to CKG.SCP.RACF, then *resource* lies in the (*access*-dependent) CKGRACF scope of *userid* in any of the following cases.

- *userid* is the owner of *resource*
- the class of *resource* is DATASET and *userid* is equal to the HLQ (High-level qualifier) of *resource*
- *userid* is SPECIAL
- *access* is READ and *userid* is OPERATIONS or AUDITOR
- the class of *resource* is USER or GROUP and *userid* is GROUP SPECIAL in some group of the group owner chain of *resource*
- the class of *resource* is USER or GROUP, *access* is READ, and *userid* is GROUP OPERATIONS or GROUP AUDITOR in some group of the group owner chain of *resource*
- the class of *resource* is neither USER nor GROUP and *userid* is GROUP SPECIAL in some group of the group owner chain of the owner of *resource*
- the class of *resource* is neither USER nor GROUP, *access* is READ, and *userid* is GROUP OPERATIONS or GROUP AUDITOR in some group of the group owner chain of the owner of *resource*
- the class of *resource* is DATASET, the HLQ of *resource* is an user or group, and *userid* is GROUP SPECIAL in some group of the group owner chain of the HLQ of *resource*
- the class of *resource* is DATASET, the HLQ of *resource* is an user or group, *access* is READ, and *userid* is GROUP OPERATIONS or GROUP AUDITOR in some group of the group owner chain of the HLQ of *resource*

Since CKGRACF is intended for administrative functions only, there is one difference between normal RACF scoping rules and CKGRACF. RACF allows a partial list of a profile to which a user has a read (or higher) permit. CKGRACF only allows full listing of profiles, and will therefore not consider these profiles within scope.

If *userid* does not have READ access to CKG.SCP.RACF, or none of the cases above holds, then the CKGRACF scope rules of the previous section come into play.

CKG.SCP.ID: the ID resource names

Table 626. ID scope profiles for CKGRACF

Class of resource	CKGRACF resource name checked
USER	CKG.SCP.ID.*userid.owner.dfltgrp*
GROUP	CKG.SCP.ID.*groupid.owner*
GENERAL	The owner of the resource is determined, and a check is done for this user or groupid.
DATASET	The owner of the data set is determined, and a check is done for this user or groupid. On failure of this check, the HLQ is taken, and a check is done for that user or groupid.

Note that if you specify an explicit user or group in an ID profile, the owner will generally not change, so "*" should suffice. Similarly, it is recommended that you use "*" for the default group, since a user is usually able to change her default group at login, and this could have unintended effects on the scope definitions.

CKG.SCP.U/G owner tree resource names

The owner tree based scope access is defined by two formats of resource names:

- CKG.SCP.U.*top.ownerx...owner2.owner1* (where *top* is a user)
- CKG.SCP.G.*top.ownerx...owner2.owner1* (where *top* is a group owned by SYS1)

For these resources, *top* is the owner of *ownerx*, *owner2* is the owner of *owner1* and *owner1* is the owner of *id* (see below).

Only one of these resources will be checked, dependent on whether *top* is a user or a group.

The *id* that is owned by *owner1* is determined as follows:

Table 627. Basic IDs for ID scope construction in CKGRACF

Class of resource	Basic id for resource construction
GROUP	The groupid itself
USER	The owner of the user profile
GENERAL	If the owner is a group, that groupid. If the owner is a user, the user's owner.
DATASET	If the owner is a group, that groupid. If the owner is a user, the user's owner. On failure of this check, the HLQ is taken and is processed similarly.

The ownership tree is travelled upwards from the basic id (see table above), until either a user or the group SYS1 is encountered. If a user is encountered, CKG.SCP.U is used, otherwise CKG.SCP.G is used. Creation of this resource happens by travelling down the ownership tree from the top id, and adding every encountered owner to the profile name.

The group SYS1 is never explicitly added to the resource, unless it's the only group in the ownership tree.

For example a user USER, has group OWNER1 as owner, which in turn is owned by group OWNER2; OWNER2 has group SYS1 as owner, thus terminating the tree. Creating the resource will form CKG.SCP.G.OWNER2.OWNER1

It is not necessary to define both SCP.ID and SCP.U/G profiles for every user and group. CKGRACF interprets a profile not found condition as denied access.

CKGRACF allows the request if either of the resources listed is permitted. We recommend that there is a high level generic CKG.** that disallows all access.

The following figure shows a simple group tree and the resulting SCP and ID resource names. A rounded box represents a user, a square box represents a group and a stretched hexagon represents a data set or general resource. The group tree shows the ownership structure, *not* the subgroup/supgroup structure. Profiles marked with *) are used only for data set resources.

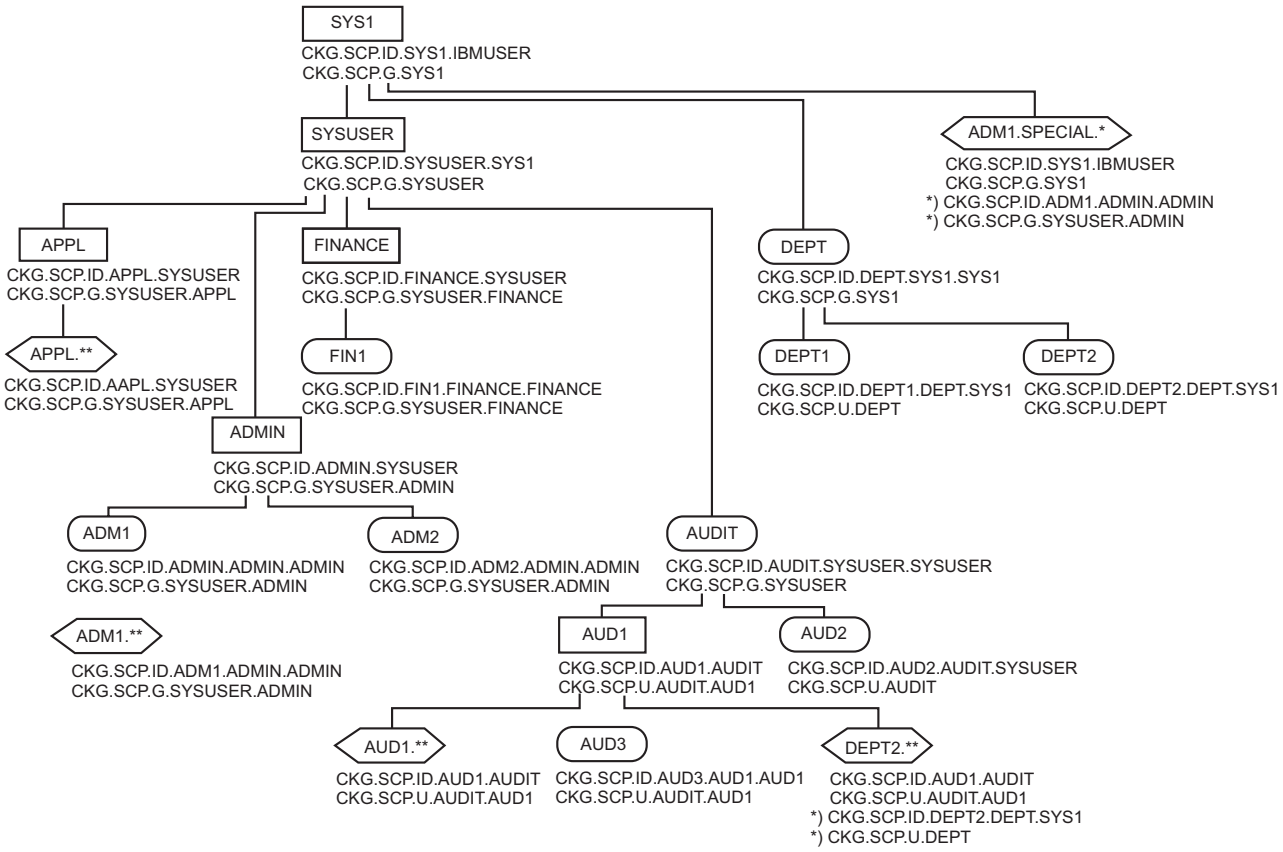


Figure 526. Group tree and scope profiles

For the group tree displayed in the preceding figure, the following scope profiles could be created:

Table 628. Examples for scope checking in CKGRACF

Profile	Comment
CKG.SCP.ID.*.ADMIN.*	All users owned by group ADMIN
CKG.SCP.ID.*.DEPT.*	All users owned by user DEPT
CKG.SCP.U.AUDIT	All users owned by user AUDIT
CKG.SCP.U.AUDIT.*	All users and groups owned 'downstream' of user AUDIT, e.g. user AUD3.
CKG.SCP.G.SYSUSER	All users owned by SYSUSER
CKG.SCP.G.SYSUSER.*	All users and groups owned 'downstream' of SYSUSER, unless the ownership is broken by a user.

Given these profiles, a scope check for user ADM2 first checks CKG.SCP.ID.*.ADMIN.*, and if access was not granted, check CKG.SCP.G.SYSUSER.*. User DEPT is not covered by any of these profiles, and is outside of any scope; access is denied to all administrators.

Permitting a user on the CKG.SCP.**.AUD1.* and the CKG.SCP.**.AUD1 profile is equivalent to giving him group-special on the AUD1 group (with regard to scope; the comments allowed can be restricted). The * and ** masks represent any number of qualifiers. So the profile matches any user below AUD1, irrespective of the groups and users between AUD1 and SYS1.

The table shows the resource names checked:

Table 629. Scope access checks for CKGRACF

Resource name checked	Access required
CKG.SCP.ID.*userid.owner.dlftgrp*	READ for LIST commands and UPDATE for all commands that modify a profile
CKG.SCP.ID.*groupid.owner*	READ for LIST commands and UPDATE for all commands that modify a profile
CKG.SCP.G.*groups...*	READ for LIST commands and UPDATE for all commands that modify a profile
CKG.SCP.U.*user.groups...*	READ for LIST commands and UPDATE for all commands that modify a profile

Restriction on scope profiles

Bear in mind the fact that the total length of a scope profile (including the prefix), can never be more than the maximum length allowed in the class these profiles are put in.

Using GLOBAL profiles

In some installations, all users are allowed to list or update their own user resource. For example, users can be allowed to LIST their own userid or to enter their own holiday schedule. While it is possible to give individual users *u* READ or UPDATE access to individual CKG.SCP.ID.*u*.** profiles, it can be more convenient to have a single profile member CKG.SCP.ID.&RACUID.**/READ or CKG.SCP.ID.&RACUID.**/UPDATE in the GLOBAL class. With such a member in place, there is no need to define individual CKG.SCP.ID.*u*.** profiles any more. Note though that if a user gets access to a resource through a member in the GLOBAL class, RACF will perform no further processing - not even auditing.

Userdata profiles

Userdata profiles can be used to set the scope for the USRDATA command. This scope check is performed only if the access check to the command profile (CKG.CMD.USRDATA) has been successful. The scope for the USRDATA command is based on the resource class, the resource owner, and the *index* (value of the USRNM field) used. The USRDATA command cannot be used to access USR entries reserved for use by CKGRACF; these have index values starting with 'CNG'. All other indices are free to be used by the installation as they see fit, e.g. an index 'PHONE'.

The scope check for the USRDATA command can have up to three steps:

- If the target profile is the current user (class is USER), or if the owner of the target profile is the current user (class is not USER), the 'own profile' resource is checked. This profile can be used to grant users access to their own profiles for a class and index value. The resource name checked is CKG.USRDATA.OWN.*class.index*. USRDATA LIST actions require READ access, other actions require UPDATE access.
- If the 'own profile' check fails or does not apply, the 'all profile' resource is checked. This profile can be used to grant system-wide access to *all* USR entries for a class and index value. The resource name checked is CKG.USRDATA.ALL.*class.index*. USRDATA LIST actions require READ access, other actions require UPDATE access.

- If the 'all profile' check fails, the 'scope profile' resource is checked. This profile can be used to grant access to the USR entries for all profiles within the CKGRACF-defined scope for a class and index value. The resource name checked is CKG.USRDATA.SCP.*class.index*. USRDATA LIST actions require READ access, other actions require UPDATE access. If this access check succeeds, the scope profiles are checked; if the scope access check succeeds also, access to the userdata is granted.

The table shows the resource names checked:

Table 630. USRDATA scope checks for CKGRACF

Resource name checked	Access required
CKG.USRDATA.OWN.*class.index*	READ for the LIST option; UPDATE for all other options
CKG.USRDATA.ALL.*class.index*	READ for the LIST option; UPDATE for all other options
CKG.USRDATA.SCP.*class.index*	READ for the LIST option; UPDATE for all other options

Racfdata profiles

Racfdata profiles are used to protect individual fields in a profile, by means of access level checks and an internal multiple-authority setting. These profiles are checked by the CMD command when parsing the RACF command given with CMD. This profile check is only performed if the access check on the command profile (CKG.CMD.CMD) was successful.

A racfdata (RAC) profile contains qualifiers for *class*, *segment*, *field*, and sometimes *value*. E.g. CKG.RAC.SCP.DATASET.BASE.ACCESS.ALT would protect the ACCESS LIST of each data set within a user's CKGRACF-defined scope. Giving a user an access of READ (or NONE) to this profile will prevent her to give other users ALTER access via the CKGRACF PERMIT command for all data sets within the scope. RACF `DATASET` profiles as indicated in the following table do not apply to CKGRACF CMD EX commands, but only to CKGRACF CMD REQ CONNECT, DELDSD, PERMIT, RDELETE, and REMOVE commands.

The access needed on a racfdata profile is READ for all commands that list a *field* and UPDATE for all commands that modify a *field*.

Access to a field is granted if and only if any of the following conditions holds:

- The current user is the target profile (class is USER) or the owner of the target profile (class is not USER), and the current user has the required access to the 'own profile' resource CKG.RAC.OWN.*class.segment.field*.
- The current user has the required access to the 'all profile' resource CKG.RAC.ALL.*class.segment.field*.
- The target profile lies within the CKGRACF-defined scope of the current user, and the current user has the required access to the 'scope profile' resource CKG.RAC.SCP.*class.segment.field*.

'Own profiles' can be used to grant users access to fields of their own profiles, while 'all profiles' can be used to grant system-wide access to fields. Similarly, 'scope profiles' can be used to grant access to fields of profiles within CKGRACF-defined scopes of users.

If access to a field is granted, the internal multiple-authority setting for the involved profile will be used to determine the actual multiple-authority of the command. When determining this multiple-authority, 'own profiles' take precedence to 'all profiles', which in turn take precedence to 'scope profiles'.

The table shows the resource names checked:

Table 631. RAC profile checks for CKGRACF

Resource name checked	**Access required**
CKG.RAC.OWN.*class.segment.field*	READ for listing the *field*; UPDATE for modifying a *field*
CKG.RAC.ALL.*class.segment.field*	READ for listing the *field*; UPDATE for modifying a *field*
CKG.RAC.SCP.*class.segment.field*	READ for listing the *field*; UPDATE for modifying a *field*

The following table shows the indexes for RAC profiles and their description.

Table 632. RAC profile descriptions for CKGRACF

CKG.RAC profiles	**Description**
class.BASE.ACCESS.READ	Checked for access set to READ
class.BASE.ACCESS.UPD	Checked for access set to UPDATE
class.BASE.ACCESS.ALT	Checked for access set to ALTER
class.BASE.ACCESS.CTRL	Checked for access set to CONTROL
class.BASE.ACCESS.NONE	Checked for access set to NONE
DATASET.BASE.ACCESS.EXEC	Checked for access set to EXECUTE
PROGRAM.BASE.ACCESS.EXEC	Checked for access set to EXECUTE
class.BASE	Checked for deletion of the access list
class.WHEN.APPCPORT	Checked for setting of conditional access for APPCPORT
class.WHEN.CONSOLE	Checked for setting of conditional access for CONSOLE
class.WHEN.JESINPUT	Checked for setting of conditional access for JESINPUT
class.WHEN.PROGRAM	Checked for setting of conditional access for PROGRAM
class.WHEN.TERMINAL	Checked for setting of conditional access for TERMINAL
class.WHEN	Checked for deletion of conditional access list
CONNECT.BASE.ADSP	Checked for turning on the ADSP flag on CONNECT
CONNECT.BASE.SPECIAL	Checked for turning on the SPECIAL flag on CONNECT
CONNECT.BASE.OPERATIO	Checked for turning on the OPERATIONS flag on CONNECT
CONNECT.BASE.AUDITOR	Checked for turning on the AUDITOR flag on CONNECT

Table 632. RAC profile descriptions for CKGRACF (continued)

CKG.RAC profiles	Description
CONNECT.BASE.GRPACC	Checked for turning on the GRPACC flag on CONNECT
CONNECT.BASE.REVOKE	Checked for setting of REVOKE flag on CONNECT
CONNECT.BASE.RESUME	Checked for setting of RESUME flag on CONNECT
CONNECT.BASE.UACC.NONE	Checked for setting of UACC NONE flag on CONNECT
CONNECT.BASE.UACC.READ	Checked for setting of UACC READ flag on CONNECT
CONNECT.BASE.UACC.CON	Checked for setting of UACC CONTROL flag on CONNECT
CONNECT.BASE.UACC.UPD	Checked for setting of UACC UPDATE flag on CONNECT
CONNECT.BASE.UACC.ALT	Checked for setting of UACC ALTER flag on CONNECT
CONNECT.BASE.OWNER	Checked for definition of OWNER on CONNECT
CONNECT.BASE.AUTH.USE	Checked for Authority USE on CONNECT
CONNECT.BASE.AUTH.CREATE	Checked for Authority CREATE on CONNECT
CONNECT.BASE.AUTH.JOIN	Checked for Authority JOIN on CONNECT
CONNECT.BASE.AUTH.CONN	Checked for Authority CONNECT on CONNECT

Schedule profiles

Schedule profiles can be used to grant access to a revoke/resume schedule for a user (see also the explanation of schedules in "USER" on page 1533). These profiles are checked for a USER SCHEDULE command; the access check is performed only if the access check to the command profile (CKG.CMD.USER.*action*.SCHEDULE) has been successful. CKGRACF checks a resource name of the form CKG.SCHEDULE.*schedule*, where *schedule* is the name of the target schedule.

The following table lists the resource name checked by CKGRACF:

Table 633. SCHEDULE profile checks for CKGRACF

Resource name checked	Access required
CKG.SCHEDULE.*schedule*	UPDATE

Schedule names must be alphanumerical and 1 to 8 characters long. A schedule profile should be created for every type of independent reason for which a user could be revoked (separation of users into groups is done using the scope profiles; there is no need to create a schedule for each decentral administrator).

For instance, at a site where the system administrator, decentral administrators, and personnel administrator are allowed to revoke and resume a userid, the schedules SYSTEM, GROUP, and PAYROLL could be used. Any administrator should have access only to the schedule that he can use. Since a user is revoked if

revoked by *any* schedule, the system administrator does not require access to the GROUP and PAYROLL profiles. We advise you to choose schedule names in a meaningful way, and create a schedule name for each type of reason a user could be revoked; e.g., use the REVOKE schedule with access for one user only to provide a 'hard' revoke. You should also create a catchall profile CKG.SCHEDULE.* with access NONE for all users, to explicitly forbid the use of undefined schedules and to allow the logging of such failed attempts.

The following table shows the profiles that should be created:

Table 634. Example of SCHEDULE profiles in CKGRACF

Profile name	**Access required**	**Meaning**
CKG.SCHEDULE.*	NONE	Catchall profile for undefined schedules
CKG.SCHEDULE.*schedule*	UPDATE	Access to schedule *schedule*

Chapter 15. Problem Determination Guide

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

Getting information for problem diagnosis

The first step in analyzing the problem is usually to obtain and save the SYSPRINT of the run. It can be accessed through the RESULTS panel (described in "RESULTS - View output and results" on page 24) or directly through the ISPF primary command SYSPRINT (unless the application crashed).

If the application has crashed and you are still in ISPF, it can usually be accessed by using

```
TSO ISRDDN
```

and looking for a CKR*x*MSG file, where *x* is the ISPF screen number. The data set name ends in `SYSPRINT`. If ISPF has also terminated, you can look for a data set under your current prefix ending in "SYSPRINT".

General problems and abends

Provided that the zSecure installation instructions are followed and all batch JCL and parameters are correctly tailored to reflect the configuration and standards at your own installation, you should not experience any problems in normal usage of zSecure. If abend codes *are* encountered when running zSecure, see Abends and other problems for further advice.

If your installation uses hot-standby volumes which are online when zSecure is being executed, see Handling hot-standby volumes for details of the SUPPRESS command, which you can use to cause zSecure to ignore those volumes.

Installations using Alternate Master Catalogs should review sections Handling alternate master catalogs and Handling catalog/VVDS inconsistencies to understand the problems which can occur in DFP, RACF, and zSecure in this type of environment.

Finally, the possibility exists that past system failures, software errors, etc. may have caused inconsistencies in the RACF database which you are unaware of but which zSecure highlights for you. Advice on the necessary actions to take can be found in Handling database layout problems.

Handling hot-standby volumes

A difficulty in the processing of zSecure is introduced by the use of *hot-standby* volumes. These volumes contain a track image copy of another volume, only the volume label is different (to be able to make the copy online). Typically, no profiles are copied. This automatically would result in a large number of error messages by the VERIFY PROTECTALL and VERIFY INDICATED functions, if discrete profiles are present for the volume. In addition, this might confuse in particular the resource deletion functionality in the MOVE, REMOVE and VERIFY commands.

For this kind of volume, zSecure provides a way to suppress all error messages and resource-oriented commands. This is done by means of the following command:

```
SUPPRESS VOLUME=volume
```

More than one command may be present indicating different volumes.

Sample output is shown in the following figure. Only the relevant sections are included in the following figure.

```
Include CKRALLOC (ISPF variable)
    2 |/* Data from DD070525 */
    3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD070525.UNLOAD'  complex=DD070525
    4 |
    6 |alloc type=IOCONFIG dsn='SYSAPPL.CNRACF.DD070525.IOCONFIG'  complex=DD070525
    7 |
    9 |alloc type=CKRCMD DD=CKR02CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
    1 |SUPPRESS VOLUME=WORKPK
    2 |VERIFY INDICATED
End of  CKRCMDV  (include level 1)

------------------------------------------------------------------------------------------------------------------------------------------------
CKR0092 00 SME003 has 1 RACF indicated dataset(s) without profile                                                                      page 4
CKR0090 00 WORKPK suppress request - 4 detail message(s) suppressed
------------------------------------------------------------------------------------------------------------------------------------------------
M E S S A G E S   V E R I F Y   I N D I C A T E D       25 Mar 2007 00:05                                                                page 5

CKR0040 04 RACF indicator set but no discrete profile found for SME003 C##BERT.SYS1.CAUNVSAM
```

Figure 527. Sample SUPPRESS VOLUME= output

Handling alternate master catalogs

Alternate master catalogs generally cause difficulties since by their purpose they provide the same function as the real master catalog. This implies that data sets cataloged in the master catalog are also cataloged in the alternate master catalog. However, VSAM data sets cataloged in multiple catalogs cause problems for DFSMSdfp, RACF, and zSecure.

For DFSMSdfp, a DIAGNOSE of the alternate master catalog will complain: the VVDS points to only one catalog, the other catalog disturbs the one-to-one relation between VVDS and catalogs.

For RACF discrete profiles, the volume name in the profile is the volume where the catalog resides, rather then the data set. Potentially, this is a security exposure if some day the alternate master catalog needs to be used - data sets that were protected by a discrete profile when they were created, are not protected anymore by this profile if the alternate master catalog is used, since the resource that RACF searches a matching profile for now contains a different volume (and of course the alternate master catalog will not reside on the same volume as the production master catalog).

For zSecure, the problem is: which profile must be considered the right one? Error messages generated for VSAM data sets cataloged in a master catalog need careful inspection. For instance, after creating a new z/OS image, page data sets are often cataloged in the wrong catalog (the one of the driving image instead of the one of the new image), or may have the wrong volume in their profiles (if you use discrete profiles).

Some problems may be addressed by using the SUPPRESS option to indicate which catalog should not be considered:

```
SUPPRESS CAT=datasetname
```

Note that the resource-handling functionality in the COPY, MOVE, REMOVE and VERIFY commands will DEFINE/DELETE catalog aliases in master catalogs as long as they are addressable from the current system (whether they are active or not) unless suppressed.

The problems can be prevented by:

- Not using the alternate master catalog, but relying on full-volume restore in case of master catalog problems.
- Not using discrete dataset profiles. Generic profiles do not contain a volume name, so they do not suffer from the preceding problems.

Handling catalog/VVDS inconsistencies

As discussed in the previous section, catalog/VVDS inconsistencies can be expected for VSAM data sets cataloged in the master catalog. Sometimes, other problems exist. Security zSecure generates error messages for these problems. These should be checked by using the IDCAMS DIAGNOSE command on the catalog and VVDS involved. Special care should be taken with these inconsistencies in relation to some VERIFY commands to identify *unused* generic or discrete profiles, and in relation to the resource deletion functionality in some MOVE, REMOVE and VERIFY commands (uncataloged non-VSAM data sets will be scratched from the VTOC, but orphan NVRs and VSAM errors will not result in any commands to remove the affected objects).

Handling VSAM on shared DASD

Shared DASD containing VSAM data sets may not be easy to understand, and zSecure contains a lot of code to help you. For each system, the normal catalog access path to be used may be different. In fact, this happens in almost all systems - primarily with data sets cataloged in the master catalog, but it might also happen because of differences in alias pointers (due to the lack of maintenance procedures that allow alias pointers to be defined in only one master catalog).

Since physically different catalog entries may describe the same data set (components) on a volume, the RACF indicated bits of VSAM clusters may be inconsistent - and the volumes to be used for a discrete VSAM profile may differ also.

Also, it may happen that components of identically named clusters on different systems *are* indeed physically different - the components may even have exactly the same name and the same volume serial. This happens for instance if multiple systems are run with their own, identically named, non-shared IPL volumes or IPL strings (IPL strings may be generated as an exact image copy of each other and then run non-shared for performance, maintenance, and availability reasons). It can even happen (although it is a threat to availability) that one cluster entry in a catalog on shared DASD is used to access two physically different, identically named components on identically named, non-shared DASD volumes.

To handle these complexities, zSecure processes a VSAM cluster name in a catalog on shared DASD for each system sharing the catalog volume, and it also processes each VSAM component on shared DASD for all systems sharing the component's volume. During this processing, the consistency of the catalog(s) with VTOC and VVDS is checked, and it is also checked whether a cluster component in a connected catalog resides in the catalog where the normal VSAM search sequence would look for it (through the system's master catalog alias matching the cluster name). If there is no system where a VSAM cluster would be found through the

normal search sequence, a message is generated. If there is no system where a cluster *component* is cataloged, a message is generated as well.

Currently, it is not fully identified *on which system* and *on which physical volume* a VSAM data set should be considered *sensitive*. This causes the REPORT SENSITIVE command to potentially report multiple copies of identically named VSAM clusters as sensitive, where actually only one of those clusters is really the sensitive one.

Handling database layout problems

Due to system failures, software errors, or other calamities, the RACF database may contain inconsistencies in its internal layout. A number of these inconsistencies is identified in error messages by zSecure. Some inconsistencies may not be intercepted, but may still provide you with unexpected output from Security zSecure.

For instance, zSecure may report on a profile that you cannot display with RACF commands. If this is the case, or if you receive messages on invalid segment identifiers or BAM block problems, you can run the RACF utility IRRUT200 to check the consistency of the database.

Typically, you find BAM block conflicts for the segments containing the profiles that are giving you problems. If you have a BAM block conflict that shows segments as allocated, while the index does not point to the segments, and zSecure erroneously processes the (partially) deleted profile, you can instruct Security zSecure to skip the profile. To do this, you must know the database number and RBA of the profile. The LIST keywords DB and RBA can help here:

```
SELECT ... /* the offending profile */
LIST CLASS, KEY, DB, RBA
```

To skip the offending profile in subsequent runs, you can explicitly exclude it from processing:

```
EXCLUDE DB=num, RBA=hexnum
```

If your problem is the other way around - you miss a profile that RACF can find but zSecure cannot find, this can only be solved by repairing the BAM block conflict with BLKUPD.

Abends and other problems

The most common system abend codes encountered with zSecure are listed in this topic along with a suggestion for the possible cause and remedy. Of course your first check should be the appropriate message manual for your operating system, that tells you the exact meaning of the abend and reason code.

001
Probably problems with blocksize. Look at the message in your job log to determine the DDname.

002
Problems with the DCB parameters of a file. Look at the message in your job log to determine the DDname. Check your specification for DCB parameters with the reference material in “Starting zSecure programs using JCL” on page 690.

30D
Access denied to load a non-controlled module while a PADS data set is open.

Typically, this happens in split-screen mode in ISPF/PDF while a zSecure display is active on the other screen. Review the messages to find which module is not controlled, and add a PROGRAM profile with NOPADCHK if you must use the application simultaneously with zSecure.

322
CPU time limit exceeded. Check the joblog for prior abend messages with a different abend code. If a prior abend occurred, solve this abend. Otherwise, increase the TIME parameter on the JOB card, code less functions together, or split the input (for example, per volume or only one RACF or ACF2 data set).

522
Check in the job log that the job was not waiting for a tape mount or offline or inaccessible device.

722
Too many output lines. Make your selection more specific or increase the output limit for your job (for instance with a /*JOBPARM L=*nn* card, where *nn* is thousands of lines allowed).

80A
878
GETMAIN error. Try to increase the REGION parameter on the EXEC or JOB card. If you have reached your site's maximum, code less functions together, or split the input (for example, per volume or per RACF or ACF2 data set).

913-74
This abend is issued for a log stream if it does not exist or if you do not have the SAF access to open it. It can also indicate other SUBSYS errors, so it is not very specific.

913
Access denied to one of the data sets. If running a batch job, review the ICH408I messages in the joblog to determine which one. If running interactively, you should have received an ICH408I message. If not, issue the TSO PROFILE WTPMSG command and try it again, you should now receive an ICH408I message.

D37
B37
One of the output data sets was too small, or there was no space left on the volume to extend the data set. Look at the message in your joblog to determine the DDname.

User Abends
Generally these errors are accompanied by a high severity message in the `SYSPRINT` indicating the specific problem and possible solutions. If this information is not included in the `SYSPRINT`, submit an error report to IBM software support.

Most abends (except some I/O related abends) are accompanied by a summary dump. For assistance on a problem by zSecure, you generally have to provide at least this summary dump, the JCL used, and the listing of the input commands.

Problems and abends in zSecure Collect

For information about CKF*xxxa* messages and abends that happen in zSecure Collect, see the *IBM Security zSecure: Messages Guide*.

Handling problems and abends in the Audit component of zSecure

This section describes problems specific to the Audit component of zSecure:

- Virtual memory requirements
- Response time problems

For information about general problems and abends, see "General problems and abends" on page 1573.

Virtual memory requirements Because of the nature of processing SMF logging data, the zSecure user must always keep in mind the size of SMF data sets, and the number of records selected in a query. The ISPF queries assume that virtual storage is large enough to store detailed information for all selected records. If you want to process a large amount of records, you should either make your query very selective (for example, select only a few records), or store less detailed information for each record selected (e.g. by specifying only a few fields on a custom query).

If zSecure is used on TSO, it can be used most efficiently using live SMF or a disk copy of the SMF data for one day. The disk copy does not need to contain all the SMF records for the day, but just the types that are being used in normal zSecure SMF queries. You can use the CKAJFUNL sample to create an online copy from the live SMF data set, or from a cumulative SMF tape.

When running a query using the ISPF interface, you need at least 5 MB virtual storage, but at least 32 MB is recommended. Large sites may need a region of 128 MB. zSecure uses virtual storage above the 16 MB line when available. If zSecure runs out of memory, SMF input file processing is terminated, and output is produced for the SMF records read until memory ran out. Early termination of SMF processing is indicated by message CKR0438 'SMF input terminated: out of memory' in the SYSPRINT file.

While a query is executing, the number of SMF records successfully processed is constantly shown. If for any reason a query should terminate because of insufficient memory, you can use the record number last shown as an upper limit and specify this number in the **Max number of records to read** field on the SMF **report parameters** panel. (See "Interactive SMF processing for RACF" on page 550.)

Alternatively, you can limit the number of SMF records selected for each group of record displays. The **Max number of records per display group** field can be used to set an upper bound to the number of records kept for each type of records.

Depending on the type of SMF records used in a query, it can save a lot of memory to disable the use of CKFREEZE data. For example, the configuration information provided through CKFREEZE data is of little use when only RACF event records are being used.

The job tag caching system is used to find the RACF or ACF2 userid for non-RACF or non-ACF2 activity records. If this option is set to YES or MINIMAL, this keeps in-storage the RACF or ACF2 userid, group, and terminal for every job when it can find this information, and uses it to complete non-RACF or non-ACF2 activity records. If set to YES, zSecure *caches* records until the record can be completed; for example, until the first SMF 30 record for the job is found. This may use several MB of memory. When memory is tight, set this parameter to MINIMAL. In this

case, records are not cached and all activity records occurring before the first SMF 30 record are not completed. Usually, these are records for jobs that were started before the begin of the SMF trace; if your SMF data is badly out of chronological order, this can occur for most jobs. If you are just reporting on RACF or ACF2 event records, you can set this option to NO in order to completely turn off the caching function. You can further tune the job tag caching system by putting an SMFCACHE command in the preamble (menu option **SE.3**).

Response time problems zSecure reports the progress of its data processing phase using ISPF messages. This helps to determine the amount of time zSecure spends in the different phases of the query. If running the query takes too long, and reading CKFREEZE data is a significant portion of the processing time, disabling the use of CKFREEZE data can speed up processing.

This might decrease the reliability of the reports. For example, it cannot find the cluster name for a VSAM component, it cannot decide if a data set is protected through a discrete or a generic profile, and it cannot find UNIX pathnames. In most instances, this does not present a problem, but in case of doubt always run your query again with CKFREEZE data.

A long response time can also be caused by excessive paging or CPU usage. In these cases, it can help to limit the number of SMF records processed for your query.

If a query takes too much time, you can interrupt SMF processing using the ATTN key. If the ATTN key is pressed, SMF input file processing is terminated. Output is produced for the SMF records read until ATTN was pressed. Early termination of SMF processing is indicated by message CKR0437 'SMF input terminated by user attention request' in the SYSPRINT file.

Creating a dump under ISPF

Standard procedure to create dumps under ISPF.

When programs running under ISPF have an abend, ISPF traps the abend and prevents any subsequent dump. If you need a dump in SYSABEND or SYSMDUMP, there are two options:

- start ISPF with the option TEST, so in linemode TSO (READY) type
  ```
  ISPF TEST
  ```
- in an existing ISPF session, type on the **Command ===>** line
  ```
  ENVIRON ENBLDUMP ON
  ```

When a program crashes, you now see a normal diagnostic dump on your terminal and the message

```
* ISPF SUBTASK ABEND *
IKJ56641I EXEC     ENDED DUE TO ERROR+
READY
```

At this point press ENTER to write a dump to SYSABEND or SYSMDUMP.

Note that the SYSUDUMP in most sites does not contain the user subpools. This makes it insufficient for problem determination.

An abending program running under ISPF can cause a follow-on abend in ISPF itself. For this reason, if you are writing a dump to a data set, make sure that the data set is allocated DISP=MOD - otherwise the dump associated with a follow-on abend will overwrite the original one.

By default, zSecure does not pass on abends to ISPF. Hence, for the purpose of creating a dump, you should specify **Pass abends to ISPF** under SETUP TRACE see "SE.T Setup - Trace" on page 1673.

Debugging menu option and action character problems

The menu options that display in the ISPF panels can be customized for the installation and also customized for individual users. The following factors determine what shows up on the menus.

- The IBM Security zSecure products installed. That is, if you have multiple products installed or different combinations of products, the menu options will be different.
- The SYS1.PARMLIB member IFAPRDxx
- The NLS tables used to translate the menus.
- Checks on resource names starting with CKR.OPTION and CKR.ACTION in the class configured in the CKRSITE module.

To troubleshoot menu issues, you can allocate a RECFM=VBA,LRECL=137 data set to file C2RIMENU. After you have allocated the file, startup data is written to the file during application startup. The data provides details about the following:

- The NLS members selected and reasons they were selected.
- The SAF checks done.
- The products that are installed.
- The menu options that are omitted because of a `PRODUCT DISABLE` statement in IFAPRDxx, or because of an unauthorized higher level menu option.
- The content of the NLS table with the NLS option with the NLS option replaced by '-' if it is not authorized.

To check action character processing, you can add a `DEBUG ACTION` statement to the preamble. This statement causes debug output for each action character to be written to the SYSPRINT file.

Support for RACF group administrators

zSecure provides support for two types of decentral administrators: group-SPECIAL administrators and decentral administrators using the CKGRACF authorized component. The program can be run so that group-SPECIAL or decentral administrators will only be able to select and display the RACF resources and profiles within their scope. In this manual, this mode of operation is called *restricted* (or less correct, *PADS mode*). Use of this option can require special zSecure configuration options, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. (The options are: PADS access to the RACF database, or restricted mode set in the CKRSITE module.)

Restricted mode can be simulated by using the SIMULATE RESTRICT command. If you include this command in your preamble (option **SE.3** from the Security zSecure menu), the program always runs in restricted mode. You can simulate restricted mode for the duration of one output list by using the NEWLIST SCOPE parameter.

When the program operates in restricted mode, a number of limitations apply and a number of commands and parameters cannot be used. These restrictions are described in the explanations for using the commands and parameters and in the command and parameter descriptions. The documentation also indicates which commands and parameters cannot be used in restricted mode.

When zSecure is operated in restricted mode, use is made of a RACF simulation engine in the product. Your local security policy might not allow you to perform *real* access control decisions based on a RACF simulation, rather than by calling RACF itself.

You can use restricted mode for your group-auditors. In restricted mode, any user is only able to select and display those SMF records relating to users or resources in his scope. Use of a CKFREEZE file is required.

Use in PADS mode

When zSecure is used in PADS mode (for example, installation-determined restricted mode, not simulated using SIMULATE RESTRICT or NEWLIST SCOPE, and not set in the CKRSITE module), a number of additional limitations caused by RACF Program Access to Data Sets apply.

- You must run the program from a 'clean' environment. This can be accomplished by running C2R (or the local copy that your installer prepared) before you start ISPF. More information on PADS mode is in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.
- You cannot operate in split-screen mode.
- You can only use program controlled STEPLIBs and ISPLLIBs. You cannot concatenate your own unauthorized libraries.

Commands not allowed in restricted mode

In restricted mode, all commands which might influence the outcome of a simulated access control decision are flagged as errors. This means that the following commands and options cannot be used:

- DEBUG except for PERFORM, RESTRICT, CPIC, ACTION, DICT, OUNIT.
- LIMIT ID and LIMIT OLD
- LIST (only forbidden with NEWLIST TYPE=RACF or outside the scope of a NEWLIST)
- NEWLIST NOEGN, NEWLIST EGN, NEWLIST SCOPE
- PRINT NOEGN, PRINT EGN
- REPORT AC1, REPORT SCRATCH, REPORT PADS, REPORT STC
- SELECT/EXCLUDE outside the scope of a NEWLIST, except when only the QUAL parameter is used. When SELECT/EXCLUDE is used within the scope of a NEWLIST, access to certain fields is prohibited.
- SHOW CLASS
- SIMULATE SETROPTS
- SUPPRESS ICHCNX00, SUPPRESS CKFREEZE (only forbidden with NEWLIST TYPE=SMF).
- SIMULATE TODAY
- UNLOAD (only forbidden with NEWLIST TYPE=RACF or outside the scope of a NEWLIST).

A number of additional restrictions apply to interactive use with ISPF:

- The REPORT and VERIFY panels only allow the use of the QUAL selection parameter. All other selection parameters cause an error.

Other limitations:

- When you use REMOVE to delete a user or group within your scope, only the access list entries within your scope are deleted. This causes orphan permits for all access list entries outside of your scope. Security zSecure generates REMOVE commands to remove connect group entries; these REMOVE commands can cause RACF to issue error messages. The DELUSER command removes the connect entries left over.
- All unprotected data sets (UACC of READ or higher) are visible. In this, Security zSecure simulates RACF. Use QUAL (REPORT, VERIFY) or a mask (DISPLAY) to view only those data sets that you are interested in.
- To get FIELD profile support, a single class and segment name must be implied by the SELECT statement.
- Segments are shown only if there is at least one field on the display/sortlist statement that the user has READ access on through the FIELD class.
- When using indexed I/O, only FIELD profiles with a non-generic class and segment name prefix are consulted.

Access allowed in restricted mode

In restricted mode, the profiles that can be selected or displayed must be in the scope of the user (for example, owned directly or indirectly, or within the CKGRACF-defined scope), or must have a UACC of READ or higher. These restrictions have been based on RACF's access decisions in ICHUT100, IRRUT100, and the LISTDSD, RLIST, and SEARCH commands: some fields require profile ownership (directly or indirectly), some fields require audit authority. Access to masked fields is not allowed.

Scoping support for non-base segments based on FIELD profiles is performed. This means formatting the fields on DISPLAY and SORTLIST statements when the user has READ access or higher on the corresponding FIELD profile, and showing modifiable fields on a DISPLAY when the user has UPDATE access or higher on the corresponding FIELD profile. For restrictions, see the previous section.

To use restricted access mode, you must either have the system-wide special or auditor attribute, or the RACF database processed must contain the userid you use to run CKRCARLA with. Your access to masked fields is determined by the authority of your userid. The following table shows the field and profile access restrictions in the four cases:

Table 635. Restricted mode: Field and profile access restrictions

Userid Authority	Access restriction
Auditor	Access to masked fields not allowed.
Special	Access to masked and global audit fields not allowed.
Group-auditor	Access to masked fields not allowed. Access to non-base segments is not allowed. Access to global audit fields not allowed except in scope of ownership. Profiles are hidden unless at least READ access. Access to access list and security level/label/category information not allowed outside scope of ownership.

Table 635. Restricted mode: Field and profile access restrictions (continued)

Other	Access to masked fields not allowed. Access to non-base segments is not allowed. Profiles are hidden unless at least READ access. Access to access list and security level/label/category information not allowed outside scope of ownership. Access to USR fields limited by the CKGRACF-defined USRDATA scope.

Support for RACF group auditors

To provide support for group-auditors, the SMF functions of Security zSecure can be used in so called *restricted mode* . Also, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide* for an explanation of restricted mode and its consequences.

Restricted mode can be in effect due to:

- Use in PADS mode , because access to the RACF database, unloaded database, CKFREEZE file, or SMF input files was granted through Program Access to Data sets, implemented as a conditional access list.
- Use of the SIMULATE RESTRICT command.
- Use of the SCOPE parameter on the NEWLIST command. In this case, the restrictions apply to the affected NEWLIST only. This only works for the SMF NEWLIST.
- A setting made in the CKRSITE module.

In restricted mode, users can only select (and display or unload) those SMF records that are in their scope. Users are allowed to see records that:

- Describe users or actions of users that are in their scope, e.g. the users owned by a group administrator. This includes the group-administrator scope defined for the CKGRACF authorized component of zSecure.
- Describe a resource that is in their scope, e.g. a data set that is owned by the user. Both data sets and general resources are supported.
- Describe a data set that is not protected (only if the system does not have ADSP or PROTECTALL(FAIL) active). Unprotected data sets are those data sets that do not have a RACF profile (discrete or generic) to protect the data set. Data sets with a UACC of READ or higher are not treated as unprotected, and are *only* visible within the user's scope.

  The visibility of unprotected data sets can be suppressed using the SUPPRESS NOPROFILE command. If this command is given, SMF records that describe an unprotected data set outside the user's scope, are not shown.

Restricted mode for the SMF processing functions of zSecure is subject to the following limitations:

- Like the restricted mode of zSecure, system-wide SPECIAL, OPERATIONS or AUDITOR is not supported in the scoping rules, but group-SPECIAL, group-OPERATIONS and group-AUDITOR is. Use restricted mode for group-administrators only.
- SMF records for which no RACF userid, RACF profile, or data set can be found can only be selected in unrestricted mode. Typically, these records describe system-wide events or status.
- The SUPPRESS CKFREEZE command is ignored, because CKFREEZE data is required to find the correct profile for data sets. The SUPPRESS reasons other than SUPPRESS NOPROFILE do not work for SMF records.

Limitations of the RACF simulation

Most VERIFY and REPORT commands are based on a simulation of the RACF access control decisions (simple LIST and DISPLAY commands are not). This simulation currently has a number of restrictions. The following RACF features are not considered in the access control simulation:

- Security levels, categories, and SECLABELs. In short, Mandatory Access Control is not yet supported (except in the COPY command).
- DASDVOL authority is not yet taken into account for access to DASD data set resources.
- The action of site-specific RACF pre- and postprocessing exits cannot be simulated. The only exit that can be handled successfully is ICHCNX00. This exit is called with a code indicating that it is ICHUT100 calling the exit. Experience shows, that not all customers using this exit have included support for ICHUT100 in their exit, and consequently zSecure also misses the support. Some sites depend on authorized features (zSecure calls the exit in an unauthorized environment), or use the current user's ACEE.
- Structural errors in the RACF database. If the IRRUT200 checks find errors, zSecure can report on profiles that cannot be found through RACF commands.

The Naming Convention Table ICHNCV00

zSecure supports the RACF Naming Convention Table ICHNCV00. A limited subset of ICHNCV00 functionality is supported in the simulation by zSecure. (Note: These programs are able to display any legal ICHNCV00 table properly, including those functions not supported by the simulation.)

In the current implementation, the following ICHNCV00 features are supported:

- Interpretation of ICHNCV00 per system; each system can have its own version of the table. For RACF reporting, the default system's ICHNCV00 is used to report on shared systems. For SMF reporting, the actual system table (as indicated by the CPU id in the SMF record) is used.
- Proper flow control using the NEXT parameter.
- SELECT and ACTION clauses using the GQ, UQ, and QUAL variables, and both numerical and literal constants. Up to 22 qualifiers with a length of up to 8 characters each are supported. Support for longer qualifiers, as used by some installations for tape data set name conversions, could be added on request.
- Subscripting of GQ and UQ using numerical subscripts. (Using implicit subscripts, or using variables as subscripts, is not currently supported.)
- Substring operations on the GQ, UQ, and QUAL variables, both in SELECT clauses and in ACTION clauses.
- SELECT clauses using RACUID, RACGPID, RACUID3, and RACGPID3. Support for this feature is limited, and always assumes a different user's and group's data set is used. In effect, this implies that comparisons using RACUID, RACGPID, RACUID3, and RACGPID3 will never match.

Restricted support is provided for the following ICHNCV00 features:

- SELECT clauses using the EVENT variable support only the RACHECK event code (X'0100').
- SELECT clauses using the VCT variable support only values of 0 (no volume specified) and 1 (one volume specified).
- SELECT and ACTION clauses using the VOLUME variable support only 1 (one volume) in VOLUME array.

- SELECT and ACTION clauses using the VOLUME variable is not supported for VSAM data sets; warning message CKR0850 is issued and no conversion takes place.
- SELECT and ACTION variables using QUAL variable also ignore the VOLUME specification; if a volume value is specified, it is ignored.

The following ICHNCV00 features are not supported:

- SELECT and ACTION clauses using any variable types other than GQ, UQ, QUAL, RACUID, RACGPID, RACUID3, and RACGPID3. Specifically, the following variable types are not supported: G, U, QCT, NAMETYPE, V, OLDVOL, WKX, WKY, WKZ, WKA, WKB, WKC.
- Data set names with more than 22 qualifiers, or with qualifiers of length zero or a length greater than 8.
- Implicit subscripting of GQ and UQ, or subscripting of GQ and UQ using variables.

SMF processing - Background

This section describes some internals of SMF processing.

At the end of each run, zSecure provides an overview of the range of records processed. For each system, the date and time of the earliest record processed and the date and time of the last record processed are shown. The sample output that follows shows the layout of the record overview:

```
CKR0452 00 SMF records were processed for the following systems:
           System ML1E from 23 Aug 1994 02:54 to 23 Aug 1994 05:10 (no CKFREEZE file)
           System ML1S from 30 Aug 1993 04:11 to 30 Aug 1993 04:14 (no CKFREEZE file)
```

Figure 528. Overview of records processed

The record overview displayed in the preceding figure does not include the date and time of SMF record types 2 and 3. These records do not describe system events, but are created by the IFASMFDP program and indicate the start time and end time of the IFASMFDP run, which is always later than the last SMF record dumped.

The date and time of the earliest and last records processed, across all systems, is also displayed in the report header.

Special processing is also performed for SMF record type 7, which indicates that SMF data was lost on the system that generated the SMF records, presumably because the SMF buffers were full. The events that occurred during the period that the SMF buffers were full are lost, and cannot be audited using SMF. zSecurebrings this to your attention using message CKR0461. (The zSecure messages are documented in *IBM Security zSecure: Messages Guide*.). The following sample shows message CKR0461:

```
CKR0461 00 48059 SMF records were lost on system  from  5 Feb 1994 00:10
```

Figure 529. Sample message CKR0461

Class, resource and profile

This section documents the way zSecure handles RACF classes, resources and profiles for the NEWLIST TYPE=SMF.

Derivation of class, resource and profile

Most RACF processing records (SMF record types 80 and 83) contain information on the class, resource, and profile processed. Most non-RACF records do not contain this information. Instead, some of these records describe data sets, from which RACF profile information can be derived. zSecure attempts to derive RACF class, resource, and profile information for data set and catalog activity records, and HSM function statistics records. It handles this in the following manner:

- The data set name is used to derive the RACF resource name. Temporary data sets are discarded: no resource name is found. For VSAM data sets, a `CKFREEZE` file might be required to find the resource name.
- The resource name is used to determine the profile name; zSecure uses the RACF database to achieve this.
- If a resource or profile name can be found, the class is set to DATASET; it is not set otherwise.

While most RACF processing records contain class, resource and profile fields, some do not. zSecure handles the exceptions in the following manner:

- The class for the RACINIT, ADDUSER, ALTUSER, CONNECT, DELUSER, PASSWORD, and REMOVE events is set to USER. The target user from the record is used as resource and profile.
- The class for the ADDGROUP, ALTGROUP, and DELGROUP events is set to GROUP. The target group from the record is used as resource and profile.
- The class for the ADDSD, ALTDSD, and DELDSD commands is set to DATASET. The resource and profile are taken from the record.
- For DEFINE events of class <>DATASET, generic profiles cannot be derived if not included in the record.
- For GENERAL events written by the CKGRACF authorized component of zSecure, the class, resource, and profile are taken from the LOGSTR field.

Example of profile derivation

As an example of the way zSecure derives the RACF information from an SMF record, let's study the fields derived for some sample RACF commands.

Assume that user USERAA, while connected to group GROUPBB, issued the command 'CONNECT XX GROUP(YY) OPERATIONS'. In that case, the following fields are set:

Table 636. Profile derivation sample field settings

Field	Value	Explanation
CLASS	USER	The class of the target profile.
EVENT	CONNECT	The event is a CONNECT command.
GROUP	GROUPBB	The current connect group of the command-issuing user.
PROFILE	XX	The target profile: user XX.
RACFCMD	CONNECT XX GROUP(YY) OPERATIONS	The full RACF command issued.
RACFCMD_GROUP	YY	The target group of the RACF command.
RACFCMD_KEYWORDS	GROUP OPERATIONS	The keywords used in the RACF command.

Table 636. Profile derivation sample field settings (continued)

Field	Value	Explanation
RACFCMD_USER	XX	The target user of the RACF command.
RESOURCE	XX	The target resource.
USER	USERAA	The command-issuing user.

If user USERAA were to issue the command DELGROUP ZZ instead, the following fields would be set:

Table 637. Profile derivation sample field settings

Field	Value	Explanation
CLASS	GROUP	The class of the target profile.
EVENT	DELGROUP	The event is a DELGROUP command.
GROUP	GROUPBB	The current connect group of the command-issuing user.
PROFILE	ZZ	The target profile: group ZZ.
RACFCMD	DELGROUP ZZ	The full RACF command issued.
RACFCMD_GROUP	ZZ	The target group of the RACF command.
RACFCMD_KEYWORDS		No keywords were used in the RACF command.
RACFCMD_USER		There was no target user of the RACF command.
RESOURCE	ZZ	The target resource.
USER	USERAA	The command-issuing user.

To summarize:

- Use the EVENT field to select specific RACF command types.
- Use the CLASS and RESOURCE fields to select the main target resource; this works for both RACF and non-RACF records.
- For user and group profiles, the RESOURCE and PROFILE fields are identical; for data set and general resource profiles, the RESOURCE field is the 'real' resource (e.g. actual data set name), while the PROFILE field can be a generic profile (e.g. 'SYS1.**').
- Use the RACFCMD or RACFCMD_KEYWORDS field to select commands using specific keywords and options.
- The RACFCMD_USER and RACFCMD_GROUP keywords can be useful to select the targets of a RACF command; in most cases, an alternative is 'SELECT CLASS=USER RESOURCE=XX'.

Use of the CKFREEZE file

zSecure can use a CKFREEZE file with catalog information to determine the resource and profile name for a VSAM data set. This is required to find the resource and profile for SMF record type 62 (some instances), type 64 (all instances) and HSM function statistics records (some instances). If no CKFREEZE file for the system is available, resources and profiles can only be found for VSAM cluster names.

zSecure always tries to read a CKFREEZE file if the CLASS, PROFILE, or RESOURCE fields are used; if this is not desired (e.g. if only RACF processing records are of interest), use the SUPPRESS CKFREEZE command.

Note: zSecure Collect, the program used to create a CKFREEZE file, does not collect VSAM path names by default. To do this requires the ALLRECS parameter in zSecure Collect. In either case, zSecure is currently unable to find resource and profile names for these data sets.

The job tag system

This section documents the way in which zSecure attempts to complete some job-related records with security package user and group information.

One of the features of zSecure is a job tag caching system; it allows zSecure to supply RACF and ACF2 userids, group ids, terminal ids and job ids for several SMF record types that do not contain this information themselves. This is accomplished by collecting all *job tags*, for example, the information that uniquely identifies a job. If the userid, group id, terminal id and job id can be found for this job tag, all other SMF records for that job can be completed with this information.

To make this system really useful, a *record cache* has been introduced. If a record is found that cannot be completed, it is stored. Processing of this record is delayed until the record can be completed or until all the input files have been exhausted. Because this feature can require a lot of memory, use the `SMFCACHE` command to limit the amount of cached records. Some record types are not cached. For those records, the missing fields are only completed if the value of these fields is obtained before the non-cached records are processed.

The job tag caching system, if active, causes the following record types to be cached and/or completed:

Table 638. Job tag system - record types to be cached or completed

Type	Description	Cached	Completed fields
14	Input Activity	Yes	All
15	Output Activity	Yes	All
17	Scratch Data Set Status	Yes	All
18	Rename Data Set Status	Yes	All
20	Job initation	No	JOBID
60	VSAM Data Set Updated	Yes	All
61	ICF Define Activity	Yes	All
62	VSAM Component or Cluster Opened	Yes	All
64	VSAM Component or Cluster Status	Yes	All
65	ICF Delete Activity	Yes	All
66	ICF Alter Activity	Yes	All
80	Racf processing	No	JOBID
83	Racf audit for data sets	No	JOBID

Table 638. Job tag system - record types to be cached or completed (continued)

Type	Description	Cached	Completed fields
92	UNIX file system activity	No	JOBID, TERMINAL

The job tag information is collected from record types 30 and 32; the job tag from any job-related record can be printed using the JOBTAG field.

Several limitations to the use of the job tag system exist. The two most important are multi-user address spaces and system address spaces. Multi-user address spaces might be a problem because RACF and ACF2 processing records might indicate the user on whose behalf an action is performed, while the job tag system indicates the user ID and group ID for job start and end records. In this case, the completed records have the address space's user ID and group ID rather than the user ID and group ID of the user causing the record to be written. Examples of such multi-user address spaces are Roscoe and FTP. System address spaces often cannot be identified uniquely. For example, address spaces that have a job name containing zeroes and the job start date and time that are also zero cannot be distinguished from one another. Because of this, records for system address spaces are ignored by the job tag system.

When your system has some long-running jobs that generate records, and you want these to be completed by the job tag system, you might have to turn on interval accounting. This option prevents the job tag system from being swamped with records that have incomplete job tags. An interval of half an hour to an hour is usually sufficient. Turn off detail recording to prevent huge CPU and I/O loads. For more information, see the information on the `SMFPRMxx`, `NODETAIL` parameter the *MVS Initialization and Tuning Guide* for more information. Use the `SMFCACHE VERBOSE` command to obtain statistics on memory usage and the amount of records cached or skipped for specific jobs.

CKGRACF Restrictions

CKGRACF has the following restrictions:

- The USR field of discrete data set profiles is not supported, see “USRDATA” on page 1554.
- If class FACILITY is used, profile keys are limited to 39 characters. The resource name checked can be up to 255 characters; however, because of the length restrictions, you might not be able to create a discrete or generic profile to fit a scope resource name checked (CKG.SCP.U... or CKG.SCP.G...).
- RACF password synchronization does not support modifications made through CKGRACF.

  RRSF propagation of CKGRACF changes can fail (with a message IRRR116I, processing code 506) if too many schedules and/or queued commands are present in the profile. Both active entries and those kept in the audit trail count towards this limit. For example, changes to USER profiles with more than 33 schedule commands with both a start and end date cannot be propagated.

  Propagation fails because the CKGRACF USRDATA becomes too long to fit into a command of 5000 bytes, which is the biggest command RRSF can propagate. The problem profile can be fixed by removing CKGRACF USR entries from it that are no longer needed with the WIPE command. See “WIPE” on page 1558, possibly followed by re-adding still relevant entries.

If the problem occurs for more than one profile, or if it re-occurs on a regular basis, the period during which CKGRACF keeps expired commands in the profiles for auditing purposes might be too long. This setting can be verified with the SHOW CKRSITE command. See "SHOW" on page 1529. If changes to this setting are needed, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Chapter 16. zSecure Collect for z/OS

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	

The zSecure Collect program, CKFCOLL gathers information about your z/OS system configuration. The program is designed to collect data quickly using minimal system resources. The data collected is analyzed by the CKRCARLA program.

To get a complete picture of your I/O subsystem, zSecure Collect must be run on all systems using shared DASD. The data can be used to provide a mapping between the physical target of I/Os on DASD and the named entity. The physical target of I/O operations can be any of the following hardware components: control unit, physical disk, cylinder, or track. The named entity is known to the user or operating system through one of the following identifiers: Device number, volume name, data set, file, data space, or PDS member). This information is necessary to perform various tasks such as:

- Matching resources (volumes, data sets, VSAM clusters) to (generic) profiles in RACF.
- Auditing the system protection by collecting information including but not limited to the following types:
  - current RACF options
  - RACF data set names
  - APF data set names
  - `LINKLIST` concatenation data sets
  - LPA list data sets
  - in-storage MLPA and PLPA members
  - page and swap data sets
  - SMF, JES2, HSM, CA1, and DMS data sets
  - SMF recording activity and exits
  - actual PPT contents
  - actual TSO command table contents
  - contents of APF data sets (AC=1 module information)
  - JES2 STC and TSU Procedure Library (`PROCLIB`) directories
  - SVC data
  - Program Call data
  - Subsystem data
  - JES2 data
  - exits
- Auditing system change. Checksum values can be computed for data sets both at member and data set level.
- Creating a system definition file for EREP (Environmental Record Editing and Printing Program), mapping errors on shared DASD to the same device (error counter).
- Creating CONFIG*xx* members for comparison between configurations.

zSecure Collect does not perform any of these functions, it only collects the data required to perform the functions. The zSecure Collect function is like the DCOLLECT function. However, the DCOLLECT function does not collect enough data to perform the resource matching, auditing, comparison, and other functions described. Consequently, you cannot use this function in place of zSecure Collect.

Other than some messages and a summary report, the zSecure Collect program does not provide reporting functions because it is designed to use minimal resources. Data analysis is done by the CKRCARLA program. You can also write your own post-processor for the collected data.

See the following topics for more information about zSecure Collect:

- "Understanding the key components of zSecure Collect"
- "Getting Started" on page 1594
- "Configuring zSecure Collect" on page 1594
- "Starting zSecure Collect" on page 1602
- "zSecure Collect command reference" on page 1612
- "zSecure Collect reports" on page 1604
- "Troubleshooting" on page 1635

Understanding the key components of zSecure Collect

When you use zSecure Collect, you need to be familiar with the following components:

- JCL to run zSecure Collect
- Input sources and the parameters
- Messages and reporting

JCL to run zSecure Collect

The SCKRSAMP library contains sample JCL to run zSecure Collect. When IBM Security zSecure has been installed and enabled, zSecure Collect can be used immediately in non-APF mode. For operations requiring APF authorization, you have to obtain a permit to the proper resource. See "Deciding whether to run APF-authorized" on page 1601 for a discussion on setting up zSecure to run with APF authorization. If you are trying out zSecure Collect for the first time, you do not need APF authorization.

Figure 530 provides sample JCL that enables data collection for zSecure Audit for ACF2, one of the products supported by zSecure Collect:

```
//CKFCOLL  EXEC PGM=CKFCOLL,PARM='FOCUS=AUDITRACF',
//         REGION=64M
//SYSPRINT DD SYSOUT=*
//CKFREEZE DD DISP=(,CATLG),DSN=userid.name.CKFREEZE,
//            UNIT=SYSDA,
//            SPACE=(32760,(1000,1000),RLSE,,ROUND)
```

Figure 530. Sample JCL to collect data for zSecure Audit for ACF2

For additional information about running zSecure Collect, see "Starting zSecure Collect" on page 1602.

Input sources and parameters

zSecure Collect can take its input from the parameter string in the JCL(PARM)statement, the SYSIN file, or both. However, neither of these sources are required. The zSecure Collect parameters and commands are used to

determine what information is collected along with other processing options. The most important parameter is the FOCUS parameter which specifies what data is collected. For example, if you specify the parameter value `FOCUS=AUDITRACF`, zSecure Collect collects data for zSecure Audit for ACF2 for RACF.

If you have the appropriate entitlements for the products, you can specify as many options as you want for the `FOCUS` parameter. The entitlements are defined in the `IFAPRD`*xx* `parmlib` member. If you do not specify any options, zSecure Collect assumes all focuses that are installed and enabled in `IFAPRD`*xx*. This default behavior means that zSecure Collect collects all data for all enabled products. If your site only uses one of the zSecure products installed, you can specify the `FOCUS` for that product explicitly. This reduces the time required for data collection time. See "Selecting the products for the collect operation" on page 1595.

For additional information about the zSecure Collect parameters and commands, see "Configuring zSecure Collect" on page 1594 and "zSecure Collect command reference" on page 1612.

Messages and reporting

zSecure Collect generates messages and one report. To understand the output data, you can review the `CKFREEZE` output. The CKFCOLL output is in a spanned variable blocked file with different kinds of records. You do not need to understand the file layout because the CKRCARLA program reads the data and processes it for you.

The `SYSPRINT` file is likely to contain messages stating that information could not be collected or is missing. These messages do not cause problems for the configuration analysis. However, the messages can be helpful to debug problems. Some messages, like `CKF017I` can be a nuisance. To suppress these types of messages, add the command `SUPMSG=17`.

Figure 531 on page 1594 provides an example of output from an authorized run. Some pages have been omitted from the sample output.

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                              page    1
 Licensed materials - property of IBM, Copyright IBM Corp. 1986-2007, All Rights Reserved

PARM:  FOCUS=AUDITRACF


CKF913I 00 Serialization has obtained all ENQs
CKF135I 00 No customer/site-specific name to be used as default CHECKPWD
           Running on SYSNAME(DINO) SYSPLEX(DINORD2R) LPARNAME(PROD) HWNAME(M3000H30)
           CPU-id 0213FF-7060
           5655-T02 IBM Security zSecure Audit for RACF

CKF182I 00 Options for this run are:
           FOCUS=(AUDITRACF)
           IO=Y,DASD=Y,TAPE=N,SWCH=N,PATH=N,VTOC=Y,VVDS=Y,PDS=Y,CAT=Y,MCD=Y,BCD=Y,DMS=Y,ABR=Y,TMC=Y,RMM=Y,VMF=Y,UNIX=Y,UNIXCLIENT=N
           RECALL=Y,AUTOMOUNT=Y,UNIXACL=Y,SHARED=Y,OFFLINE=N,SMS=Y,STATS=N,IDR=N,CHECK=N,SCAN=Y
           PARALLEL=PATH,REPORT,KEY0,BYPASS,SIO,XMEM,XMDSN,DIAG,UID0,ENQ=Y,IOTIMEOUT=60,PDSEBUFSIZE=150
           SERIALIZATION(ENQ(CKRDSN),FAIL)

CKF047I 00 Data collection started on  6 Jun 2007 13:43 for node JES2DINO sysname DINO     sid DINO netid NLCRMM04
           on a IBM 7060 model P30
           MVSCP configuration id 09  logical partition PROD      sysplex DINORD2R
CKF039I 00 Running IBM CORP z/OS 1.4.0 DFSMS 1.3.0 JES2 z/OS 1.4
           VTAM 6.1.4/ESA  RACF 7.7.7  RMF  7.1.2    TSO 3.3.0     HSM  1.5.9
CKF130I 00 SMS system DINO configuration SMS=00 BASE SCDS
CKF002I 04 LOCATE return code 8 on SMS managed APF dataset CRMA.APFLOAD
CKF111I 00 Scheduler allocated 3 I/O executors
CKF330I 08 system abend 806-04 (module invalid or could not be found) returned by LOAD of exit IGG019E4 from 20A6 SM3008 CRMA.CRMTES
CKF248I 04 OPEN abend 213-04 on device 209F volume SM3001 for CRMQARUN.APF.NONEXIST
CKF190I 00 Slowdown mode invoked because VVDS SYSP01 has no index entry for SYSP01  SYSP.RMM.P1.CDS

CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                              page    3
Volume overview

Storgrp  Volume  Dev    VTOCtrk read  DSCB#  VSAM ISAM nonVSAM  F3 VVDStrk read  recs CAT ix data slw trks   recs PDS no trks dirblk
DEMO     DEMOU1 210A  S |    60   22    776    14         719    41|    30    3    732|    1    1       10    1388|
DEMO     DEMOU2 210B  S |    60   22    761    23         716    20|    30    4    738|
         DINOP1 2031  S |    60    6      5     2           1      |    30    1      2|
         DINOP2 2032  S |    60    6      5     2           1      |    30    1      2|
         DINOP3 2033  S |    60    6      5     2           1      |    30    1      2|
         DINOSY 2030  S |    60    9    187   119          66      |    30    2    119|    2    2        9    1536|    5     14    7
         ECAM01 23FE  S |    60    6      3                 1      |                   |
         ECAM02 23FF  S |    60    6      3                 1      |                   |
EPR      EPRPAG 2091  S |    30    5    106     4          98     2|    10    1    101|
EPR130   EPR13H 2092  S |    60    7     46    15          28     1|    30    1     42|    1    1        2      35|
-------------- ( cut away ) --------------------
total             281      14950 2663  56901  7624       47660  1055|  6170  319  23033|   84   92   1 2683  277298|  154    244  482
                      .S. Shared DASD
                      ..C CP-formatted volume
-------------- ( cut away ) --------------------
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                              page   19
Summary

CKF297I 00 Number of allocations: static 4 dynamic 283, freed 0, max allowed 1,635 due to TIOT SIZE(32)
CKF008I 00 Number of DASD devices interrogated: 281
CKF009I 00 Number of DSCB entries copied: 56,901
CKF010I 00 Number of VVDS datasets processed: 225
CKF011I 00 Number of NVR/VVR entries copied: 23,033
CKF041I 00 Number of catalogs processed: 93
CKF042I 00 Number of BCS records copied: 113,998
CKF142I 00 Number of MCD records copied: 100,062
CKF143I 00 Number of BCD records copied: 57,187
CKF226I 00 Number of RMM control records copied: 6,051
CKF035I 00 Number of PDS directories processed: 201
CKF307I 00 Number of UNIX directory entries copied: 116,653 from 13,555 directories in 64 file systems
CKF338I 00 Number of UNIX ACL records copied: 42 access ACLs, 4 directory default ACLs, 0 file default ACLs
CKF034I 00 CKFCOLL used 41.0 CPU seconds, 158 elapsed seconds, and collected 108.960 MB (0.691 MB/s)
           Written 511,063 records to CKFREEZE C#MASCH.HCKR181.CKFREEZE on SM3013
           Region requested 131,072KB, granted 11,176+131,072KB
           max used in jobstep 612+2,012KB
```

Figure 531. zSecure Collect sample output

Getting Started

To run zSecure Collect, you need to configure the program and then start the collection process. Before beginning the configuration process, review "Understanding the key components of zSecure Collect" on page 1592 for an overview of the zSecure Collect program. For instructions, see the following sections:

- "Configuring zSecure Collect"
- "Starting zSecure Collect" on page 1602

Configuring zSecure Collect

The zSecure Collect program supports several types of commands that help manage program operation and customize the amount and type of data collected. For more information, see the "zSecure Collect command reference" on page 1612. See the following topics for information and instructions for configuring zSecure Collect.

- "Managing program operation using environment variables."
- "Selecting the products for the collect operation"
- "Using APF-only parameters to restrict some APF-authorized collection" on page 1597
- "Setting the collect parameter options (Feature=)" on page 1596
- "Specifying alternate data sources" on page 1597
- "Restricting information collection using SELECT and EXCLUDE commands" on page 1598
- "Reducing disk space required for data collection" on page 1600
- "Verifying the operating system where zSecure Collect runs" on page 1601.
- "Deciding whether to run APF-authorized" on page 1601.
- Specify general options such as `CAPS` and `REPORT`. See "zSecure Collect command reference" on page 1612.

Managing program operation using environment variables

You can use the `IF`, `APF`, and `EXIT` commands to manage the operation of zSecure Collect. For example, you can stop the run if the program is not APF authorized, or if the job is run on an unintended system. You can use the `IF`, `APF`, and `EXIT` commands to stop the run when the program is not APF authorized. It also stops the program if the job is run on an unauthorized system. You can even tailor the exact parameters used in the run based on the static system symbols defined on the system.

Selecting the products for the collect operation

The information collected is determined by the *focus* explicitly selected using the `FOCUS` parameter, or implied by the products installed and the `PRODUCT` statements in `IFAPRD`*xx*. Based on these specifications, some information is collected by default. You can also specify additional parameters to change the default collection process or to collect additional information. To use a specific `FOCUS`, the following prerequisites must be fulfilled:

1. The corresponding product must have been purchased and installed.
2. The product must not be disabled in PARMLIB member `IFAPRD`*xx*.
3. If zSecure Collect is running APF-authorized, you must be *permitted* by the System Authorization Facility (SAF) to use each of the focuses specified. SAF can return three levels of authority: *access allowed*, *access unexplained*, and *access prevented*. You must be explicitly authorized to access the `CKF.`*`focus`* resources in the CKRSITE-defined class corresponding to the selected focuses. There are exceptions to this rule: `TSIEM` and `ALERT` SAF authorizations are not needed if the `AUDIT` focus is also requested. `VISUAL` SAF authorization is not needed if RACF focus is also requested.

The focus can be specified by the parameter `FOCUS`. If it is not specified, the value defaults to the products that have been enabled. If you have only one product for which zSecure Collect gathers data, you can omit the parameter. The exception to these focus rules is for the zSecure Alert product. If you have this product, you must always explicitly specify `FOCUS=ALERT`.

Figure 532 on page 1596 provides an overview of the default settings–dependent on APF status, and supported features for each focus.

```
Y - Default =YES and allowed to specify =NO
. - Default =NO or 0 and NOT allowed to specify another value
n - Default =NO  and allowed to specify =YES
v - Default =0   but value specification is allowed

parameter <--------------- focus ----------------->
          ADMIN     AUDIT     TCIM/ALERT VISUAL
          Napf apf  Napf apf  Napf apf   Napf apf
ABR       Y    Y    Y    Y    .    .     Y    Y
ALLOC     Y    Y    Y    Y    Y    Y     Y    Y
BCD       .    Y    .    Y    .    .     .    Y
CAT       .    Y    .    Y    .    Y     .    Y
CICS      Y    Y    Y    Y    Y    Y     Y    Y
CHECK     .    .    n    n    .    .     .    .
DB2       Y    Y    Y    Y    Y    Y     Y    Y
DMS       Y    Y    Y    Y    .    .     Y    Y
IDR       .    .    n    n    .    .     .    .
IMS       Y    Y    Y    Y    Y    Y     Y    Y
INTERVAL  .    .    .    .    .    .     .    .
MCD       .    Y    .    Y    .    .     .    Y
MONITOR   .    .    .    .    .    .     .    .
OFFLINE   n    n    n    n    n    n     n    n
PATH      .    .    .    .    .    .     .    .
PDS       n    Y    n    Y    n    Y     .    .
RECALL    Y    Y    Y    Y    Y    Y     Y    Y
RMM       Y    Y    Y    Y    .    .     .    .
SCAN      .    .    Y    Y    .    .     .    .
SHARED    Y    Y    Y    Y    Y    Y     Y    Y
SIGVER    n    Y    n    Y    n    Y     .    .
SMS       Y    Y    Y    Y    Y    Y     Y    Y
STATS     .    .    .    .    .    .     .    .
SWCH      .    .    .    .    .    .     .    .
TAPE      .    .    .    .    .    .     .    .
TCPIP     .    Y    .    Y    .    Y     .    .
TMC       Y    Y    Y    Y    .    .     .    .
UNIX      .    .    Y    Y    Y    Y     .    .
VMF       Y    Y    Y    Y    .    .     .    .
VTOC      Y    Y    Y    Y    Y    Y     Y    Y
VVDS      Y    Y    Y    Y    Y    Y     Y    Y
```

Figure 532. Features allowed by focus type (focus = product code)

Use the column corresponding with the first part of the focus name (for example, use the AUDIT column for AUDITRACF).

Setting the collect parameter options (Feature=)

To control the type of information to be included, feature selection commands are available. These commands are of the type *feature*=YES/NO. Most of the features are only valid under specific focuses. Specification of YES if the focus does not entitle the feature results in error message CKF134I. You can also specify NO independently of the current focus and serves to suppress collecting data of the specified type.

The features are more or less *hierarchical*. If some features are set to *NO*, it implies the NO setting for a number of features at a lower hierarchical level. This propagation is done after all input has been read and all IF statements have been processed. Figure 533 on page 1597 lists the dependencies for the zSecure Collect feature selection commands. For complete documentation on the zSecure Collect commands, see “zSecure Collect command reference” on page 1612.

```
N - Specified as NO
a - Default N, alternate data source allowed
n - Default N, Y or alternate data source allowed
Y - Specified as YES
. - Default Y or N depending on FOCUS/APF

Parm specified:
IO        N    .    .    .    .    .    .
UNITIO    .    N    .    .    .    .    .
ALLOC     .    .    N    .    .    .    .
DASD      .    .    .    N    .    .    .
VTOC      .    .    .    .    N    .    .
VVDS      .    .    .    .    .    N    .
CHECK     .    .    .    .    .    .    Y

Implies:
ABR       N    N    n    n    .    .    .
ALLOC     N    N    N    Y    Y    Y    Y
CAT       N    N    N    n    n    .    .
CHECK     N    N    .    .    .    .    Y
MCD       N    N    a    n    .    .    .
BCD       N    N    a    n    .    .    .
DMS       N    N    a    n    .    .    .
IDR       N    N    .    .    .    .    Y
PATH      N    N    .    .    .    .    .
PDS       N    N    a    n    .    .    .
RMM       N    N    a    n    .    .    .
SCAN      .    .    .    .    .    .    .
SIGVER    N    N    a    n    .    .    .
SWCH      N    N    .    .    .    .    .
TAPE      N    N    .    .    .    .    .
TCPIP     .    .    .    .    .    .    .
TMC       N    N    a    n    .    .    .
UNIX      N    N    N    .    .    .    .
VMF       N    N    n    n    .    .    .
VTOC      N    N    N    n    N    .    .
VVDS      N    N    N    n    N    N    .
```

Figure 533. Feature selection commands - dependencies

Using APF-only parameters to restrict some APF-authorized collection

These following options are primarily meant to aid in problem determination and problem circumvention during APF-authorized runs: `NOSIO`, `NOBYPASS`, `UNCONNECTED`, `NOKEY0`, `NODIAG`, `NOUID0`, `NOXMEM`, and `NOXMDSN`. For details on these parameters, see "zSecure Collect command reference" on page 1612. All options specifically disable some APF-authorized ways of obtaining information. Generally, you do not need to specify any of them.

Specifying alternate data sources

These options are meant to select the data set names of additional data sources. For example, these options are used for selection when you have more than one HSM or DMS system active, when you need additional PDS directories, or when zSecure Collect fails to determine the required data set name automatically. Automatically generated data set names requires access to all data sets. Data set names specified manually, using the data source parameters only require access to the SAF resource if the program is running APF-authorized. However, *manually* coded data set names do require a READ access on the data set with one exception: With access to the SAF resource, zSecure Collect can dump any PDS directory without having access to the data set.

You can use the following alternate data source parameters to specify data set names: PDSDIR, ICFCAT, HSMMCD, HSMMCDS, HSMBCD, HSMBCDS, DMSFILES, DMSUNL, DMSPARMS, TMCDSN, RMMCTL, ARCDSN, VMFDSN, CHECK, and CHECKDSN.

If no explicit volser has been supplied for these alternate data sources, they might not be found if the volume does not get processed for other reasons. To ensure that the data sources can be found, you can specify the RECALL=YES setting. This option explicitly allocates all data sets with an unknown volser, but also recalls migrated data sets. Or, you can specify the VTOC=YES setting which forces the program to read all volumes in order to dump their VTOCs.

Restricting information collection using SELECT and EXCLUDE commands

The SELECT and EXCLUDE commands can be used to select data on either the device or volume level and on the data set level. You can use the SELECT and EXCLUDE commands to reduce the number of records written to the CKFREEZE file commands by including or excluding information by *device* or *volume* or by *data set level*. These commands can only be used to reduce the number of records written to the CKFREEZE file. They cannot be used to select extra records beyond the selections implied by the FOCUS parameter settings and other zSecure Collect options.

You can use one or more SELECT and EXCLUDE commands to restrict data collection. Multiple SELECT statements on the same level imply an *inclusive or* function. For each selection level, the commands are processed in the following sequence.

1. Select commands are processed first.
   - If a SELECT command is present and the selection criteria of all SELECT commands *fail*, the current candidate is skipped and no further processing is performed.
   - If the SELECT options are met, any EXCLUDE options present are processed.
   - If all the EXCLUDE commands fail, the current candidate is selected and is included; otherwise it is skipped.
2. EXCLUDE commands are processed next.

   If all the EXCLUDE commands fail, the current candidate is selected and included; otherwise the candidate is excluded.

Use the following base syntax to specify the SELECT and EXCLUDE commands. Use these commands with the device or data set level options as required.

SELECT= *list*
SEL=*list*
S=*list*
The SELECT command accepts a list of selections enclosed in parentheses and separated by commas. If only one selection option is needed, the parentheses can be omitted. The selections in the list indicate an AND condition if they are on the same level; multiple commands indicate an OR condition.

EXCLUDE= *list* **EXCL=***list* **X=***list*
The EXCLUDE command accepts a list of selections enclosed in parentheses and separated by commas. This syntax applies to all commands with more than one format. If only one selection option is needed, the parentheses can be omitted. The selections inside the list indicate an AND condition if they are on the same level; multiple commands indicate an OR condition.

For details on how to use these commands to restrict the data written to the CKFREEZE file, see the following sections:

- "Selecting data by device or volume"
- "Selecting data by data set level"
- "Examples of device and data set level selections" on page 1600

Selecting data by device or volume

Use the following options for selecting or excluding data at the device or volume level. For examples, see "Examples of device and data set level selections" on page 1600.

Device/volume level selection options

CH= *xx*
CHP=*xx*
CHANNEL=*xx*
C=*xx*
Restricts selection to the devices on a specified (physical) channel (path). The channel must be specified as two hexadecimal digits.

VOLUME= *xxxxxx*
VOLSER=*xxxxxx*
VOL=*xxxxxx*
V=*xxxxxx*
Restricts selection to the devices which have a volume serial starting with the specified string. The value can be 1 - 6 characters long.

DEV= *xxxx*
DEVICE=*xxxx*
UNIT=*xxxx*
U=*xxxx*
Restricts selection to the devices which have a device number starting with the specified string (1 - 4 hexadecimal digits). Both 3 and 4 character names are checked. For example, U=123 would select device 123, 0123, 1230, 1231, 1232, and so on.

STORGRP= *xxxxxxx*
SG=*xxxxxxx*
Restricts selection to the devices belonging to the specified storage group (1 - 30 characters).

LCU= *xxx*
Restricts selection to the devices which are members of the specified logical control unit. This parameter applies to MVS/XA and MVS/ESA sites not running under VM. The LCU number of a device group is available from RMF reports and IOCP reports. The LCU must be specified as 3 hexadecimal digits, or as a prefix for LCU names of 1 or 2 hexadecimal digits.

Selecting data by data set level

For the devices selected through device level selection, the data set level selection regulates which records are to be dumped. See "Selecting data by device or volume." Data set specific records are only written if they match any data set selection criterion that has been specified. For example, only VTOC, VVDS, ICF catalog, and HSM MCDS and BCDS records are dumped for the specified data set. If you want to dump information contained in a data set, use options like `PDSDIR` or one of the options ending in DSN, like `CHECKDSN`. Use these options instead of the `SELECT=DSN=` specification.

Use the following options when selecting data by data set level. For examples, see "Examples of device and data set level selections" on page 1600.

DSNHLQ= *list*
The DSNHLQ command accepts a list of HLQs, enclosed in parentheses and separated by commas. If only one HLQ is needed, the parentheses can be omitted. This option can be used to select or exclude data sets that have an HLQ specified in the list.

DSN= *prefix* **DSNPREF=***prefix* **D=***prefix*
Restricts selection to the data sets that have a name starting with the specified string. This option is like the DSNHLQ option. The use of DSNHLQ is preferred to DSNPREF, especially since it is much faster with larger selections.

Examples of device and data set level selections

For examples of device and data set level selections, review the following code examples.

An example of a selection option to collect information for one LCU only:

```
SELECT=LCU=005
```

The same example, but excluding a specific volume giving problems:

```
SELECT=LCU=005
EXCLUDE=VOL=DISK12
```

An example to select a number of volumes based on their prefix, abbreviated as much as possible (logical OR):

```
S=V=SSD
S=V=SHR
```

An example to select a number of volumes based on both their volume serial prefix and their SMS storage group (logical AND):

```
SEL=(VOL=OVFL,STORGRP=PRIMARY)
```

An example of a selection option to collect information for all data sets with HLQs SYSS, SYSP, and SYSQ:

```
S=DSNHLQ=(SYSS,SYSP,SYSQ)
```

Reducing disk space required for data collection

`CKFREEZE` data sets can become large because of the amount of data collected. You can conserve disk space and reduce CPU processing time) by turning off `CKFREEZE` features that are not required for day-to-day tasks. You can also save disk space by using SMS compression for the `CKFREEZE` data set.

Disabling the following features can reduce the necessary disk space drastically. Disable these features when the resulting `CKFREEZE` records are not required for your daily tasks.

BCD=NO
The Backup Control Data set data is currently only used for determining if discrete data set profiles need to be removed. These discrete data set profiles are found in various AU.V - Verify functions and are reported in the RACF profiles report (RA.3.1). If you do not use any discrete data set profile or run the RACF profiles report often, you can disable this function.

This information is used in `VERIFY ONVOLUME` and `REPORT_PROFILE NEWLIST`.

UNIX=NO
UNIX data requires substantial amounts of disk space (all directories, owner

data, and file permissions are stored). UNIX data is used for TRUSTED reports, SENSITIVE data sets reports (HFS data set sensitivity), and auditing UNIX filesystems. SMF records pertaining to UNIX files often do not contain the path to the file, and the CKFREEZE information can be used to show the appropriate path. Without the UNIX data, most reports still give usable, though incomplete, results. When you are not auditing the HFS or zFS data sets, turn off this feature.

This information is used in the following NEWLIST types: UNIX, TRUSTED, REPORT_SENSITIVE, DSN, SENSDSN, and SMF.

SMS compression can also reduce the amount of disk space needed to store the CKFREEZE data sets. To use this compression, in SMS you must create a DATACLAS for the CKFREEZE data sets with COMPACTION option set to YES. Examine whether compressing the data sets improves overall performance. Reading a compressed data set uses less I/O but can require more CPU.

Verifying the operating system where zSecure Collect runs

The features included in zSecure Collect make the data heavily dependent on the operating system version in effect during the data collection. Check to see if you are running a current and supported release at http://www.ibm.com/software/support/lifecycle/index_a_z.html.

Older releases (including OS/390, MVS/XA and MVS/ESA but not MVS/370 and MVS/SP1) probably work for most options, but are no longer fully tested. The zSecure Collect program has been designed to tolerate changes in the operating system without ending the program. Instead of ending the program, some record types are left out if the program does not know how to find them. When this problem occurs, a message is sent to the user.

Deciding whether to run APF-authorized

zSecure Collect provides support for both authorized and unauthorized operation.

To run authorized, copy the program to an APF library and run from this library. You must also define the profiles or rules for the CKRSITE-defined class in your security system. This definition determines who can use which authorized functions through the System Authorization Facility (SAF). Unless sufficient authority is granted to the proper resource, the program refuses to operate with APF authorization. Access is authorized if RACSTAT returns *inactive* or *not installed*. If this problem occurs, a message is issued to indicate that no authorization checking was possible and why.

Callers that want to run the program without having access to the proper resource must drop the APF authorization. For example, authorization requirements can be dropped by running it from a non-APF library, or by including a non-APF library in the STEPLIB.

The program issues a message if it is run without authorization, to note the reason for missing information. Clearly, not all configuration information can be obtained if the program is run without authorization. Specifically, APF authorization provides the following benefits:

- DFSMS requires authorization to read the VVDS data set. The VVDS is used to report cluster names instead of system-generated names VSAM component names. The VVDS is required by IBM Security zSecure if VSAM data set protection has to be taken into account.

- DB2, CICS, and IMS data is obtained by zSecure Collect from the address space private region only if you are running zSecure Collect APF-authorized.
- The Communications Server requires APF authorization to read the TCP/IP stack configuration data.
- Security and integrity can be enhanced for zSecure Collect operations by removing the following requirements: Remove the `READ` access requirement to APF libraries for directory dumps. Remove the `ALTER` access requirement to APF libraries for dumping ICF catalogs. This function requires APF to bypass the data set protection and is authorized for all focuses that permit dumping these data sets.
- VM data is obtained only if you are running APF-authorized. This processing applies to all focuses.
- Information is obtained from the following sources: The JES2 address space provides information about the procedure libraries in use for started tasks and TSUs, the spool data set name, and parameter data set and member names. The HSM address space provides information about the migration and backup control data set names being used. Use of this function is authorized only if the ID in use is explicitly authorized to access the corresponding focus resource.
- Information is obtained from the JES2, HSM, and VTAM address spaces on the current setting of security sensitive parameters (like command authority and exits).
- Information is obtained from the RMF address space, for instance RMF release. Use of this function is authorized with all focuses.
- Information is obtained about TCP/IP stack configuration.
- Information is obtained about the CS Resolver configuration.
- A test is done to see whether the device is responsive before trying to allocate it. This check prevents volumes reserved by other operating systems from hanging. Use of this function is authorized with all focuses.

When any or all of the benefits of APF authorization are considered essential, you might want to specify the `APF` keyword. Specifying this keyword causes the program to end with a return code of `12` when authorization cannot be obtained. In addition, a `CKFREEZE` file is created with only a zSecure Collect identification record. Using the `APF` option saves considerable time and resources compared to the creation of a `CKFREEZE` that contains only limited data.

Note: As with any authorized program, it is recommended that you install the program on a test system first.

Starting zSecure Collect

You can start zSecure Collect by using the **F** (Refresh) transaction for the **Setup Input files** (**SE.1**) option. See Table 647 on page 1647. This transaction submits a job that runs zSecure Collect as a batch process. However, for production purposes zSecure Collect is normally run using job C2RJPREP. Copy this job to your batch job scheduling system, and customize it with your naming conventions and other local requirements. For details, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Calling zSecure Collect using JCL

The call interface to CKFCOLL, the main zSecure Collect module, can follow the convention used for the JCL EXEC statement as well as the TSO command calling interface (CPPL). Note, however, that authorized execution from TSO requires an entry in the authorized command or authorized program list (IKJTSO*xx*). The following list describes the ddnames and file names that are supported.

SYSPRINT
Lists messages and statistics. The record format is set by default to `VBA` for non-`SYSOUT` files, and to `VA` for `SYSOUT` files. However, record formats `V`, `VB`, `F`, `FB`, `VA`, `FA`, `VBA`, and `FBA` are all supported. The record length defaults, depending on the record format, yield a printable line length 132. With the default `VBA` record format, this would yield 137 for the LRECL. A shorter line length (79 for example) is possible but results in truncation of some headers, messages, and report lines. If you do not specify a block size, a suitable default is chosen.

SYSTERM
Lists status messages and messages with a severity of 8 or higher. These messages are also printed on `SYSPRINT`. This file can be omitted.

CKFREEZE
All configuration information is written to a sequential file in VB or VBS format with a minimum `LRECL` of *23472*. The default is *VBS*.

The `LRECL` specified limits the length of VVDS and catalog records copied. If no `LRECL` is specified, then the `LRECL` value defaults to *X* which means that the record length is unlimited for VBS files and (`BLKSIZE - 4`) for VB files. You do not need to specify a value for `BLKSIZE` because the system can automatically determine the optimum block size for the device you are using.

ISPF shows the JCL specification `LRECL=X` as `LRECL=32768`. LRECL=X does *not* imply that records are 8 bytes longer than 32760. It implies support for multi-segmented records which are those records longer than 32K. Truncating these records to 32760 removes more than 8 bytes. For catalogs this processing behavior can explain the missing connector entries. If you have to process these data sets with utilities like file transfer, do not truncate `CKFREEZE` data sets after they have been created as part of the file transfer process. Instead, specify a smaller `LRECL` value like 32760 when you create or fill the data sets. zSecure Collect correctly folds records that exceed the `LRECL`. Do not terse a VBS `CKFREEZE` file.

The required space is approximately 2 megabytes per online DASD volume.

The CKFREEZE file can be a striped or compressed data set to increase postprocessing program throughput or to reduce space requirements.

Instead of allocating the `CKFREEZE` ddname in the JCL, an existing `CKFREEZE` data set name can also be allocated through the `CKFREEZE=dsn` parameter.

SYSIN
This file can contain parameters. They are described in the next section.

Sample JCL included is listed in “Getting Started” on page 1594.

zSecure Collect reports

zSecure Collect automatically generates reports on the collected information. To suppress reports, specify the NOREPORT option for zSecure Collect.

To view a report sample and list of field descriptions, see the following topics.

- "Volume overview report"
- "Partitioned data set overview" on page 1606
- "Catalog and VSAM CHECK overview" on page 1608
- "Migration, tape catalog, PDS/E, and non-VSAM CHECK overview" on page 1609
- "UNIX mount point overview" on page 1611
- "Summary report" on page 1612

Note: To limit the size of the samples, lines have been deleted from the reports.

Volume overview report

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                          page    3
Volume overview

Storgrp  Volume  Dev    VTOCtrk read  DSCB#  VSAM ISAM nonVSAM  Ext VVDStrk read  recs CAT ix data slw trks   recs PDS no trks dirblk
LARGE90  SM3010 2082  S     60   17    421    11          391    17     30    3    403          1       42    4004
PRIME90  SM3011 2083  S     60   17    379    11          350    16     30    3    361                                1       1
PRIME90  SM3012 2084  S     60   13    316     8          286    20     30    2    293
PRIME90  SM3013 2085  S     60   16    405     5          378    20     30    2    382                                5       5     1
LARGE90  SM3014 20C0  S     60   13    250     2          235    11     30    2    236
         STK001 2081  S     60    8    133     7          124           30    1      7    1    1        2     126
         SYSJ00 202A  S     60    6      5     1            2           30    1      1
SYSP     SYSP00 2028  S     60   11    255    48          193    12     30    2    240    2    2     1498  120214
SYSP     SYSP01 2029  S     60   14    251    71          147    31     30    3    227    1    1   1   10    6342
         SYS100 2022  S     60    6     14     4            8           30    1      5         1        6     165
         SYS102 202B  S     60    6     23     3           16     2     30    1      4         1      271   43296
         TMP30B 20AA  S      1    1      4                 2
TESTSYS  TSTRES 2300  S     30    6    167    34          128     3     10    2    167    2    2       11     796
TESTSYS  TSTUS1 2301  S     30   13    453     5          428    18     10    2    418
         VMSYS1 0346  SC
         ZOSNP1 220F  S     60    6      9     2            5           30    1      2
         ZOSNR1 2210  S     60   11    290    19          269           10    1     21    1    1        3      89
         ZOSNR2 2211  S     60   16    534   123          409           10    2    123
         ZOSNR3 2212  S     60    6     14                 12
         ZOSNSY 220E  S     60    8    139    71           64     2     30    1     71    2    2        5     875
ZOSN     ZOSNU1 220D  S     60    8    137    17          111     7     30    1    121    1    1        2      72
         Z140R1 2016  S     60   12    315     9          304           30    1     11    1    1        3      94    50     99  276
         Z140R2 2017  S     60   16    519   125          392           30    2    125                                43     74  163
         Z140R3 2018  S     60    6     21     7           12           30    1      7
         Z2CIC1 030E  S     29    7    208    39          167           30    1     39    1    1        1     188
         Z2DB21 0315  S     29   12    454   246          206           30    3    246
         Z2DIS1 0312  S     29    9    324     7          315           30    1      7
         Z2DIS2 0313  S     29    3     37    19           16           30    1     21
         Z2DIS3 0314  S     29   12    463    47          414           30    1     50
         Z2RES1 030F  S     29   10    361     1          355     3     30    1      1
         Z2RES2 0310  S     29   12    467    24          441           30    1     24
         Z2USS1 0311  S     29    3     19     1           14     2     30    1      1
         Z2WAS1 0316  S     29    3     47     9           36           30    1      9
         Z2WAS2 0317  S     29    3     28     4           22           30    1      4
         Z4CIC1 2207  S     29    7    228    43          183           30    1     43    1    1        2     184
         Z4DB21 2208  S     29   12    474   258          213     1     30    3    258
         Z4DIS1 2213  S     29    9    311     7          302           30    1      7
         Z4DIS2 2214  S     29    3     14     7            5           30    1      9
         Z4DIS3 2215  S     29   12    453    37          414           30    1     37
         Z4DIS4 2216  S     29    6    196    67          127           30    1     67    1    1       11    2481
         Z4RES1 2209  S     29   11    399     1          371    25     30    1      1
         Z4RES2 220A  S     29   12    490    24          456     8     30    1     24
         Z4USS1 220B  S     29    3     18     1           15           30    1      1
         Z4WAS1 2205  S     29    3     40     8           30           30    1      8
         Z4WAS2 2206  S     29    3     29     5           22           30    1      5
         Z5CCC1 225B  S     60   10    237    43          192           30    1     43
         Z5CIC1 2221  S     29    7    245    49          192     2     30    1     49    1    1        1     217
         Z5DB21 2220  S     29   11    429   274          153           30    3    274    1    1        4     577
         Z5DB22 2228  S     29    6    163     7          154           30    1      7
         Z5DB81 2227  S     29   11    423   258          163           30    3    258    1    1        3     426
         Z5DIC1 2255  S     60   13    367    19          346           10    1     19
         Z5DIC2 2256  S     60    6     39    13           24           30    1     14
total             192       9162 1780  42535  5233       36192   726   4600  222  13396   56   64   1 2046  208137   150    253  540
                     .S. Shared DASD
```

Figure 534. zSecure Collect Volume Overview report

Table 639. zSecure Collect Volume overview Report - field descriptions

Column	Meaning
Storgrp	SMS Storage group or blank if none

Table 639. zSecure Collect Volume overview Report - field descriptions (continued)

Column	Meaning
Volume	Volume serial
Dev	Device address
VTOCtrk	Number of tracks allocated for VTOC
read	Number of VTOC tracks read
DSCB#	Number of DSCBs selected from VTOC
VSAM	Number of format 1 DSCBs with VSAM data set organization (components) including the counts for both format-8 DSCBs and format-1 DSCBs.
ISAM	Number of format 1 DSCBs with ISAM data set organization
nonVSAM	Number of non-ISAM, non-VSAM format 1 DSCBs
Ext	Number of format-3 DSCBs and format-9 DSCBs (indicates multiple extents)
VVDStrk	Number of tracks allocated to the VVDS
read	Number of VVDS tracks read
recs	Number of NVR and VVR records selected
CAT ix	Number of non-imbedded indices on the volume processed with EXCP
data	Number of ICF or HSM catalog data components on the volume processed with EXCP
slw	Number of ICF or HSM catalogs on the volume processed with VSAM GET
trks	Number of tracks read from the ICF or HSM catalog data components on the volume using EXCP
recs	Number of ICF and HSM catalog BCS records selected
PDS no	Number of partitioned data set directories on the volume processed with EXCP
trks	Number of tracks read from PDS directories on the volume
dirblk	Number of directory blocks read from partitioned data sets on the volume

In addition, the volumes can be flagged with up to three, one-letter flags. The legend for these flags is printed below the report if any of the flags was present. The following flags can appear:

Table 640. zSecure Collect Volume Overview Report - Volume flag indicators

Flag	Meaning
V.. Non-dedicated VM device	Virtual device under VM.
R.. Read-only	Read-only VM device.
T.. T-disk	VM temporary disk.
.S. Shared DASD	The volume has been generated as shared.
..N No VTOC on volume	Volume did not have VTOC at IPL time.
..C CP-formatted volume	Volume is in a format suitable for VM.
..A AIX-formatted volume	Volume is in a format suitable for AIX/ESA.

Table 640. zSecure Collect Volume Overview Report - Volume flag indicators (continued)

Flag	Meaning
..L Linux partition found	The VTOC contains at least one Format 1 DSCB for a Linux partition. This flag is only shown if the VTOC has been read.
..O Other OS (Amberjack)	The VTOC F4 DSCB indicates it is formatted for a non-z/OS Operating System (`Amberjack` volume). This flag is only shown if the VTOC has been read.
..U Unsupported VTOC	Volume Table of Contents format not recognized
..M VTOC moved	VTOC not on same track as during last mount.
..T I/O Timeout	I/O to the volume timed out, possibly in use by other system
..I Invalid or missing VTOC index	The volume has no valid VTOC index.

Partitioned data set overview

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                    page    4
Partitioned data set overview

Data set name                                Dev  Volume type    trks   read members dirbl A flags
CCISCV1.IDMS8902.STARTUP.LOAD                 3CA SYST10 PDS        3      1             1 R            APF
CCISCV2.IDMS8902.STARTUP.LOAD                 3CA SYST10 PDS        3      1             1 R            APF
C#MA.C#MPROD.LOAD                             3CA SYST10 PDS      463      1             6 R            APF
C#MA.C#MTEST.LIBRARY                          3C6 PRIM16 PDSE       1                    1 R            APF
C#MA.C#MTEST.LOAD                             3CA SYST10 PDS       28      1             2 R            APF
C9103.LOADLIB1                                3CA SYST10 PDS        5      1             3 R            APF
IPO1.LINKLIB                                  3D9 M93113 PDS       61      1             5 R            APF
IPO1.LINKLIB                                  3C8 S9311A PDS       61      1             5 R            APF     Lnk
M9311.TUD.VTAMLIB                             3C7 M93110 PDS        3      1             3 R            APF
N9311.SSPLIB                                  3CA SYST10 PDS      167      1             9 R            APF
RDAO.ENGINE.LOAD                              3C2 PRIM12 PDS        2      1             1 R            APF
RDOP.CDSLIB                                   3CA SYST10 PDS        1      1             1 R            APF
RDOP.OLTLIB                                   3CA SYST10 PDS      284      6           237 R            APF
RDOPMCS.MICS.VCCLOAD                          3CA SYST10 PDS       69      1             3 R            APF
RDOPROB.UNB.NJEIP.LOAD                        3CA SYST10 PDS       28      1             1 R            APF
RDPSCV1.IDMS8902.STARTUP.LOAD                 3CA SYST10 PDS        3      1             1 R            APF
RDPSCV2.IDMS8902.STARTUP.LOAD                 3CA SYST10 PDS        3      1             1 R            APF
SYSAPPL.AMDAHL.OLTEC.R20A.L14A.R43L.LOAD      3C6 PRIM16 PDS      273      2            59 R            APF
SYSAPPL.CNRACF.CNRLOAD                        3CA SYST10 PDS      138      1             1 R            APF
SYSAPPL.MEMOREX.LMS217.LOADLIB                3CA SYST10 PDS      170      2            54 R            APF
SYSAPPL.SUPSESS.V146.CUM9301.LOADLIB          3CA SYST10 PDS       64      3           102 R            APF
SYSAPPL.UCLA1410.APFLOAD                      3CA SYST10 PDS        9      1             2 R            APF
SYSAPPL.UCLA1500.APFLOAD                      3CA SYST10 PDS        3      1             1 R            APF
SYS1.CICS9103.CICSLPA                         3CA SYST10 PDS        1      1             1 R                LPA
SYS1.CMDLIB                                   3C8 S9311A PDS       62      2            47 R            APF     Lnk
SYS1.CNMLINK                                  3C8 S9311A PDS      303      4           150 R            APF     Lnk
SYS1.CSSLIB                                   3C8 S9311A PDS        7      1            31 R            APF     Lnk
SYS1.DGTLLIB                                  3C8 S9311A PDS      128      2            78 R            APF     Lnk
SYS1.DIVERSEN.LINKLIB                         3CA SYST10 PDS       40      1             8 R            APF     Lnk
SYS1.GDDMLOAD                                 3C8 S9311A PDS      229      2            63 R            APF     Lnk
SYS1.ISAMLPA                                  3C8 S9311A PDS       16      1            19 R            APF
SYS1.ISFLOAD                                  3C8 S9311A PDS       10      1             4 R            APF     Lnk
SYS1.ISFLPA                                   3C8 S9311A PDS        1      1             1 R            APF LPA
SYS1.ISPLOAD                                  3C8 S9311A PDS       16      1            17 R            APF     Lnk
SYS1.ISPLPA                                   3C8 S9311A PDS       45      1             6 R                LPA
SYS1.ISRLOAD                                  3C8 S9311A PDS       58      1            10 R            APF     Lnk
SYS1.ISRLPA                                   3C8 S9311A PDS      277      1            24 R                LPA
SYS1.JSX.LOAD                                 3C8 S9311A PDS       10      1             3 R            APF     Lnk
SYS1.LINKLIB                                  3C8 S9311A PDS     1452     11           456 R            APF     Lnk
SYS1.LINKLIB.#00                              3C8 S9311A PDS        1      1             1 R            APF     Lnk
SYS1.LPALIB                                   3C8 S9311A PDS      664      7           291 R                LPA
SYS1.MIGLIB                                   3C8 S9311A PDS      179      4           148 R            APF     Lnk
SYS1.M9311.TUD.VTAMLIB                        3C8 S9311A PDS        3      1             3 R            APF
SYS1.NCPLIB                                   3CA SYST10 PDS      863      1             2 R            APF
SYS1.NUCLEUS                                  3C8 S9311A PDS      329      2            75 R            APF     Lnk
SYS1.PLICOMP                                  3C8 S9311A PDS       45      1            10 R            APF     Lnk
SYS1.PLILINK                                  3C8 S9311A PDS       76      2            61 R            APF     Lnk
SYS1.PROCLIB                                  3C8 S9311A PDS       25      1            18 R                        Proc
SYS1.PROCLIB.#00                              3C8 S9311A PDS        1      1             1 R                        Proc
SYS1.PRODUCTS.LINKLIB                         3CA SYST10 PDS      230      2            69 R            APF     Lnk
SYS1.SAMPMSG1                                 3C8 S9311A PDS        7      1             3 R            APF     Lnk
SYS1.SAMPRUN2                                 3C8 S9311A PDS        3      1             1 R            APF     Lnk
SYS1.TEST.LINKLIB                             3C8 S9311A PDS                              N Not found  APF
```

Table 641. zSecure Collect Partitioned data set overview report - field descriptions

Column	Meaning
Data set name	Name of the partitioned data set

Table 641. zSecure Collect Partitioned data set overview report - field descriptions (continued)

Column	Meaning
Dev	Device address of data set
Volume	Volume serial of data set
type	PDS for DSNTYPE=PDS or PDSE for DSNTYPE=LIBRARY
trks	Size of data set in tracks (1 for PDSEs, regardless of actual size)
read	Number of tracks read from directory and members using EXCP
members	Number of members read using EXCP (or BPAM, for PDSEs)
dirbl	Number directory blocks copied
A	The access that the user running the job has on the data set: None, Read, Update, Control, or Alter (blank without an AUDITRACF, AUDITACF2, or AUDITTSS focus).
flags	PDS attributes. The following attributes are reported: **Not found** Data set not found in VTOC. **Not mounted** Volume was not mounted or it was excluded. **APF** Data set is part of Authorized Program Facility list. **LPA** Data set is part of the link pack area list. **Lnk** Data set is part of LNKLST concatenation. **Proc** Data set is a JES2 procedure library. **Check** Checksum computation requested for all members. **Mismatch** Data set was not a PDS but requested as such.

Catalog and VSAM CHECK overview

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                    page    5
Catalog overview

Data set name                          Dev  Volume IX blk  CISZ ext DA blk  CISZ CAtk ext  trks read records  flags
AEP1UCAT                               0EE4 SYAEP1   1024  1024   1   1024  1024        1                    Unconnected
CSD0UCAT                               04CD CICSD0   1024  1024   1   1024  1024        1                    Unconnected
DSYCAT.MVS530.MC.EMVCAT                0307 EMVCAT   1024  1024   1   1024  1024    3   1    60   10    1259 Mstr
DSYCAT.MVS530.MC.IPL1PK                     IPL1PK                                                            Notfound
DSYCAT.MVS530.MC.SMC01F                0107 SMC01F   1024  1024   1   1024  1024    3   1    60   12    1248
DSYCAT.MVS530.UC.EMVSYS                0302 EMVSYS    512   512   1  10240 20480   14   1    30    1       7
DSYCAT.MVS530.UC.FMVT02                0100 FMVT02    512   512   1  14336 28672   14   1    30    1       7
DSYCAT.MVS530.UC.PROD01                041C PROD01   4096  4096   1   4096  4096   14   1   360   52    9362
DSYCAT.MVS530.UC.PROD02                011C PROD02   4096  4096   1   4096  4096   14   1   435  141    9969
DSYCAT.MVS530.UC.PROD03                031B PROD03   4096  4096   1   4096  4096   14   1   360   81    5928
DSYCAT.MVS530.UC.SDSK01                0401 SDSK01   4096  4096   1   4096  4096   14   1    60    1       4
DSYCAT.MVS530.UC.SYS301                0400 SYS301   4096  4096   1   4096  4096   14   1   165    1       4
DSYCAT.MVS530.UC.SYS302                0404 SYS302   4096  4096   1   4096  4096   14   1   165    1       4
DSYCAT.MVS530.UC.SIMS01                0407 SIMS01   4096  4096   1   4096  4096   14   1   120    1       4
DSYCAT.MVS530.UC.SMD89D                0304 SMD89D    512   512   1  10240 20480   14   1    30    1      35
DSYCAT.MVS530.UC.SMS001                0305 SMS001    512   512   1  10240 20480   14   1    30    1      37
DSYCAT.MVS530.UC.TSO301                0411 TSO301   4096  4096   1   4096  4096   14   1   435    1      17
OD03UCAT                               06BA PROD03   1024  1024   1   1024  1024    2   1   120    1       9
OD05UCAT                               04C5 PROD05   1024  1024   1   1024  1024        1                    Unconnected
OD10UCAT                               04CE PROD10   1024  1024   1   1024  1024    2   1   120    1       4
OD13UCAT                               04CA PROD13   1024  1024   1   1024  1024    3   1   120    1       6
OD01UCAT                               0C23 POD901   1024  1024   1   1024  1024        1                    Unconnected
F101UCAT                               0EE1 SYF101   4096  4096   1   4096  4096   14   1   135   71    7716
G001UCAT                               0D76 SPG001    512   512   1   4096  4096        1                    Unconnected
I001UCAT                               0EEA SYI001   1536  1536   1   4096  4096        1                    Unconnected
I201UCAT                               0D77 SYI201   1024  1024   1   1024  1024    2   1   120    6     429
SYSHSM.P.BCDS                          03CE SYS002   2048  2048   1  12288 12288   14   1  4500 1632   69211 BCD Nospan
SYSHSM.P.MCDS                          03CE SYS002   2048  2048   1  12288 12288   14   1  3000 1134   58958 MCD Nospan
SYSRMM.IPO1.CONTROL                    03CE SYS002   2048  2048   1  10240 10240   14   1   330  212   17533 RMM Nospan
```

Figure 535. zSecure Collect Catalog and VSAM CHECK overview report

Table 642. zSecure Collect Catalog and VSAM CHECK overview report - field descriptions

Column	Meaning
Data set name	Name of the catalog data component
Dev	Device address of data component
Volume	Volume serial of data component
IX blk	Index physical block size (bytes)
CISZ	Index control interval size (bytes)
ext	Number of extents for index
DA blk	Data component physical block size
CISZ	Data component control interval size (bytes)
CAtk	Number of tracks per control area for data component
ext	Number of extents for data component
trks	Number of tracks in use for data component (based on high used RBA)
read	Number of tracks read from data component using EXCP
records	Number of records selected from data component

Table 642. zSecure Collect Catalog and VSAM CHECK overview report - field descriptions (continued)

Column	Meaning
flags	Catalog attributes. The following attributes are reported: **Notfound** Volume not mounted. **Range** Key range data set (deprecated feature) **Repl** Sequence set replication (deprecated feature). **Imbed** Imbedded index (deprecated). **Nospan** Non-spanned data component. **Unconnected** No connector entry found in master catalog. **MCS** HSM Migration Control Data set. **BCD** HSM Backup Control Data set. **RMM** RMM Removable Media Manager control data set. **Mstr** Master catalog. **CHCK** VSAM data set requested on the CHECK statement. **+C** Catalog that has also been requested on the CHECK statement.

Migration, tape catalog, PDS/E, and non-VSAM CHECK overview

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                          page    6
Migration, tape catalog, and PDS/E, and non-VSAM CHECK overview

Data set name                          Dev  Volume Type   Blksz Lrecl │ Trks  used  read │A Records volumes profiles data sets
C#MA.C#MTEST.LIBRARY                   03C6 PRIM16 PDSE   4096       │                  │R       1                              
DSYSYS.NONIBM.ABR.ARCHIVE              0133 CRM004 ABR   27872 27872 │ 1500  1500   270 │R     270                        46511
DSYSYS.NONIBM.CA1.TMC                  0404 SHRM02 TMC     200   200 │ 1950  1806  1806 │R  119196   42574              40673
DSYSYS.NONIBM.DMS.AUTHLIB              030A DMS101 DMSA   6080    80 │                  │R      15                              3
DSYSYS.NONIBM.DMS.DMSPARMS             030A DMS101 PDSM   6080    80 │                  │R      53                             
DSYSYS.NONIBM.DMS.FILES                030A DMS101 DMSF  27998       │ 1275  1275   945 │R                              108538
```

Figure 536. zSecure Collect Migration, tape catalog, PDS/E, and non-VSAM CHECK overview report

Table 643. Migration, tape catalog, PDS/E, and non-VSAM CHECK overview - field descriptions

Column	Meaning
Data set name	Name of the data set
Dev	Device address of data set
Volume	Volume serial of data set

Table 643. Migration, tape catalog, PDS/E, and non-VSAM CHECK overview - field descriptions (continued)

Column	Meaning
type	Type of data set. The following types are available: **ABR** FDR/ABR Archive control data set. **CHCK** Data set requested on the CHECK statement. **+C** Data set that has also been requested on the CHECK statement. **DMSF** DMSFILES data set. **DMSU** Unloaded DMSFILES data set. **PDSE** PDS/E directory. **PDSM** PDS member, DMS AUTHLIB. **TMC** CA1 Tape Management Catalog. **VMF** CA-TLMS Volume Master File.
Blksz	Physical block size from format 1 DSCB
Lrecl	Logical record length (LRECL) from format 1 DSCB
Trks	Number of tracks allocated for data set
used	Number of tracks in use for data set
read	Number of tracks read using `EXCP` (for PDSEs: number of directory blocks read using BSAM)
A	The access that the user running the job has on the data set. Any of the following values can be listed: *None*, *Read*, *Update*, *Control*, or *Alter* (blank without an AUDITRACF, AUDITACF2, or AUDITTSS focus).
Records	Number of records read
volumes	Number of volume records copied to `CKFREEZE` file
profiles	Number of RACF profile coding records copied to `CKFREEZE` file
datasets	Number of data set records copied to `CKFREEZE` file

UNIX mount point overview

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                          page    7
UNIX mount point overview

Data set name                                Volume Directories  Failed    Files  with ACL Mount point
UNIXR8.ROOT                                  UNIX01         870              15455          /
UNIXR8.ETC                                   UNIX01          86                426          /etc
/TMP                                                          1                  6          /tmp
C##BOMVS.U.HFS                               SM3002         125                418          /u
*AMD/u/automount                                              1                  4        1 /u/automount
C##BOMVS.U.C##AROB.HFS                       SM3001           1                  9       47 /u/automount/c##arob
C##BOMVS.U.C##ASCH.HFS                       SM3002          13                224          /u/automount/c##asch
C##BOMVS.U.C##BAHI.HFS                       SM3004          14                225        5 /u/automount/c##bahi
C##BOMVS.U.C##BEPRD.HFS                      SM3009           1                  2          /u/automount/c##beprd
C##BOMVS.U.C##BERT.HFS                       SM3002          43                331          /u/automount/c##bert
C##BOMVS.U.C##BGUS.HFS                       SM3005           1                  4          /u/automount/c##bgus
C##BOMVS.U.C##BJTI.HFS                       SM3005           1                  6          /u/automount/u/automount/c##bjti
C##BOMVS.U.C##BLU1.HFS                       SM3001        6256              28089          /u/automount/c##blu1
C##BOMVS.U.C##BMR1.HFS                       SM3004           2                 32          /u/automount/c##bmr1
C##BOMVS.U.C##BMR2.HFS                       SM3006           1                  2          /u/automount/c##bmr2
C##BOMVS.U.C##BMU1.HFS                       SM3003           1                 11          /u/automount/c##bmu1
C##BOMVS.U.C##BOON.HFS                       SM3004        1893              16039          /u/automount/c##boon
C##BOMVS.U.C##BPK1.HFS                       SM3003           1                  2          /u/automount/c##bpk1
C##BOMVS.U.C##BTKR.HFS                       SM3002           1                  3          /u/automount/c##btkr
C##BOMVS.U.C##BVC1.HFS                       SM3006          44                586          /u/automount/c##bvc1
C##BOMVS.U.C##BVC2.HFS                       SM3002           1                  2          /u/automount/c##bvc2
C##BOMVS.U.C##QA.HFS                         SM3003           2                100          /u/automount/c##qa
C##BOMVS.U.C##QARA.HFS                       SM3001           1                  3          /u/automount/c##qaRacfwin
C##BOMVS.U.C##8090.HFS                       SM3005          33                540          /u/automount/c##8090
C##BOMVS.U.C2EAUDIT.HFS                      SM3005          23                392          /u/automount/c2eaudit
C##BOMVS.U.C2RNEW.HFS                        SM3008         142               2484          /u/automount/c2rnew
                                                                 1                          /u/automount/c2rserver
C##BOMVS.U.C2RSRV#P.HFS                      SM3003          20                381          /u/automount/c2rsrv#p
C##BOMVS.U.NFS.HFS                           SM3003           1                  2          /u/automount/nfs
C##BOMVS.U.RCCSL01.HFS                       SM3004           4                 53          /u/automount/RCCSL01
C##BOMVS.U.CNR250.HFS                        SM3007          36                436          /u/automount/CNR250
C##BOMVS.U.C2RSRV#P.RCW2201.UPG.HFS          SM3001          26                455          /u/automount/C2RSRV#P
C##BOMVS.U.PR91241.HFS                       SM3003           9                158          /u/automount/PR91241
*AMD/u/automount2                                             1                  2          /u/automount2
C##BOMVS.U2.C##QADIR.HFS                     SM3009           5                 19          /u/automount2/c##qadir
C##BOMVS.U2.NOSECUR.HFS                      SM3009         603               4821          /u/automount2/nosecur
SYSP.UNIX.P1.PERL5.HFS                       SYSP00          43                544          /usr/lib/perl
SYSP.UNIX.P1.USRLOCAL.HFS                    SM3005          88               2039          /usr/local
```

Figure 537. zSecure Collect UNIX mount point overview report

Table 644. UNIX mount point overview - field descriptions

Column	Meaning
Data set name	Name of the UNIX File System data set that was mounted at the mount point.
Volume	Volume serial of data component. This column shows *client* when the file system is a UNIX File System of another system that is connected through XCF.
Directories	Number of UNIX directories read from the UNIX File System data set.
Failed	Number of directories that could not be read. This column shows `client=n` if the file system is a UNIX File System of another system that is connected through XCF, but collection was not requested (parameter UNIXCLIENT=N was specified) . The Directories and Files columns are blank in this case.
Files	Number of directory entries read from the directories.
with ACL	The number of files in the file system that have an access ACL. This column shows `unixacl=n` if the file system did contain any access ACLs, but collection was not requested.
Mount point	Absolute path name of the mount point for the UNIX File System data set

Summary report

```
CKFCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                page   8
Summary

CKF008I 00 Number of DASD devices interrogated: 192
CKF009I 00 Number of DSCB entries copied: 42,535
CKF010I 00 Number of VVDS datasets processed: 162
CKF011I 00 Number of NVR/VVR entries copied: 13,396
CKF041I 00 Number of catalogs processed: 65
CKF042I 00 Number of BCS records copied: 83,910
CKF142I 00 Number of MCD records copied: 77,552
CKF143I 00 Number of BCD records copied: 42,662
CKF226I 00 Number of RMM control records copied: 4,013
CKF035I 00 Number of PDS directories processed: 163
CKF307I 00 Number of UNIX directory entries copied: 91,474 from 12,770 directories in 56 file systems
CKF338I 00 Number of UNIX ACL records copied: 53 access ACLs, 6 directory default ACLs, 4 file default ACLs
CKF560I 00 Number of CICS regions interrogated: 1, Transactions: 95, Programs: 263
CKF561I 00 Number of IMS regions interrogated: 3, Transactions: 67, PSBs: 133
CKF034I 00 CKFCOLL used 25.8 CPU seconds, 153 elapsed seconds, and collected 83.337 MB (0.545 MB/s)
           Written 390,665 records to C#MASCH.C2F160.CKFREEZE on SM3013
           Region requested 65,536KB, granted 11,176+65,536KB
           max used in jobstep 476+1,672KB
```

The summary report is always printed and gives an indication of the number of volumes and different kinds of records collected.

zSecure Collect command reference

The zSecure Collect program supports a number of parameters and commands that either restrict the information collected to a subset of your I/O subsystem, or that collect information for a specific purpose. Some restrictions are more limiting than others, and some restrictions can be combined to generate a subset. This section provides detailed information about each parameter and command including option descriptions, default settings, and any product-related restrictions. For example, some commands are available based on which products are installed and activated in your environment. For an overview of the commands supported by product feature, see Figure 532 on page 1596.

For details on the configuration and collection process, see "Getting Started" on page 1594 and "Configuring zSecure Collect" on page 1594.

Command syntax

You can specify the zSecure Collect parameters on the PARM field of the `EXEC` statement, or in the SYSIN file.

- Multiple parameters can be specified, separated by commas, semicolons, and/or blanks. The commands are not case-sensitive.
- If the `SYSIN` file is 80 characters wide, only positions 1 - 72 are read.
- Commands can be continued on the next line, but not in the middle of a word.
- The line end acts as a separator just like a blank or comma.
- If parameters are specified more than once, the value last given is used.
- Parameters on the `EXEC` statement or passed on a TSO command are processed before the parameters in the SYSIN file.
- All parameters are listed on the `SYSPRINT` file, prefixed with their origin (`PARM` or `SYSIN`).
- The *command order* is free, except that the `FOCUS` command must be specified before any command that is not permitted under each focus. Practically speaking, `FOCUS` should either be the first command or be omitted altogether.
- To indicate a comment, use `/*` at the beginning of the comment, and end the comment with `*/`.
- If not already part of such a comment, `*` also starts a comment, which then runs to the end of the line

Command parameters

zSecure Collect supports the following parameters.

ABR

Use this parameter to specify whether you want ABR archive records to be collected from the active Automatic Backup and Recovery (ABR) archive control file as defined in the LNKLST concatenation or STEPLIB module FDROPT.

ABR=NO
Specify *NO* to suppress collecting ABR archive records. This setting is implied by FOCUS=ALERT* and TCIM* if no other focuses are present.

ABR=YES
Specify *YES* to collect the ABR archive records. This value is implied by FOCUS=ADMINRACF, AUDIT*, and VISUAL, and is *only* valid under these focuses. If running under RACF with an AUDIT* focus but not APF authorized, the program only opens the archive control file automatically if the user has READ authority to it.

ALLOC

Use this parameter to manage the input and output for DASD devices.

ALLOC=NO
Specify *NO* if you only want to permit explicitly solicited I/O to DASD devices. If you use this setting, the following values are implied for the specified zSecure Collect parameters: DASD=N, PDS=N, MCD=N, BCD=N, CAT=N, TMC=N, DMS=N, RMM=N, VMF=N, UNIX=N, ABR=N. Consequently, you cannot set the values of these parameters to Y.

This setting does not prevent I/O to explicitly requested data set names. Neither does it prevent I/O to tape devices or ESCON switches which is what differentiates ALLOC=NO from UNITIO=NO. The CKFREEZE file includes all device numbers and volume names, but not the physical ids necessary to map (shared) DASD, nor the contents of any VTOC, VVDS, catalog, UNIX file system, or PDS.

ALLOC=YES
Specify *YES* (behind an IF command, for example) to negate the meaning of a previous ALLOC=NO statement.

ALLRECS

Use this parameter to request all ICF catalog, HSM MCDS and HSM BCDS, and RMM control records instead of a subset of record types used by zSecure products.

APF

Use this parameter to specify that APF authorization is considered essential. For example, you can specify the APF parameter when specific information is needed that requires the authorization granted by running APF. If authorization cannot be obtained, the program terminates with RC 12 and create a CKFREEZE file that only contains a zSecure Collect identification record. For a detailed discussion on authorization and when it is needed see "Deciding whether to run APF-authorized" on page 1601.

ARCDSN

The syntax for this command is:

ARCDSN= *dsn*
ARCDSN=dsn/vol

Use this parameter to request that the archive of the specified Automatic Backup and Recovery (ABR) archive control file be included in the CKFREEZE file. This parameter is only supported for FOCUS=ADMINRACF, AUDIT*, and VISUAL. Also see "Specifying alternate data sources" on page 1597.

AUTOMOUNT

Use this parameter to specify whether CKFCOLL causes an automatic mount for UNIX file systems that are not currently mounted.

AUTOMOUNT=NO
Specify *NO* if you do not want the UNIX files systems to be automatically mounted.

AUTOMOUNT=YES
Specify *YES* if you want UNIX file systems that are not currently mounted to be automatically mounted. This value is the default setting if UNIX=YES is specified or implied.

BCD

Use this parameter to specify whether to collect information from the active HSM Backup Control Data set.

BCD=NO
Specify *NO* if you do not want the HSM Backup Control Data set to be collected. This value is implied by FOCUS=ALERT* and TCIM* if no other focuses are present.

BCD=YES
Specify *YES* to request collection of the HSM Backup Control Data set information. This value is implied by FOCUS=ADMINRACF, AUDIT*, and VISUAL and permitted *only* under these focuses. It is *only* honored if the program is running APF-authorized, because APF authorization is needed to determine the data set name. Also, the HSM address space must be swapped in.

BURST parameters

Use the BURST parameters to manage the operation of I/O bursts.

BURSTS

The syntax for this parameter is BURSTS= *nn*.

Use this non-APF option to modify the number of I/O bursts done in an attempt to access a device along all its paths. The default value is 20.

BURSTWAIT

The syntax for this parameter is BURSTWAIT= *nn*.

Use this non-APF only option to modify the number of centiseconds waited between bursts. Specify a time period that gives a reasonable chance that an active I/O has terminated. The default value is 50.

BURSTSIZE

The syntax for this parameter is BURSTSIZE= *nn*.

Use this non-APF option to modify the number of I/Os in a burst done in an attempt to access a device along all its paths. It should at least be equal to the maximum number of paths to any device. The default value is 4.

CAPS

Use this parameter to request capitalization of output messages. This parameter does not affect the first page header or the parameter listing of previous parameters.

CAT

Use this parameter to manage the behavior of catalog data dumps. You can specify the following settings:

CAT=MCAT
Specify *MCAT* to cause the master catalog (but no user catalogs) to be dumped. All password fields in all records are overwritten with bytes containing hex EF to prevent security exposures. This parameter is only permitted if `CAT=Y` is permitted.

CAT=NO
Specify *NO* to suppress catalog dumps.

CAT=YES
Specify *YES* to cause the master catalog and all ICF user catalogs pointed to by the master catalog to be dumped. However, all password fields in all records are overwritten with bytes containing hex EF to prevent security exposures. It is the default when running APF authorized.

CHECK parameters

Use the CHECK parameters to determine whether you want checksum (*fingerprint*) computation to be done.

CHECK=DD

The syntax for this parameter is `CHECK=({DD|DDPREF}=` *`dd`*`)`.

Specify this value to request checksum, or fingerprint, computation for data sets. This is sometimes called *freezing*. All data sets allocated to the specified ddname, or matching the prefix on the `DDPREF`, are read and two checksum computations are performed: one for global comparison, and one for change control audit or virus detection. (The latter requires a user-specific CHECKPWD parameter.) The checksum for each data set in a concatenation is performed separately. For PDS and PDSE data sets selected with this method, checksum values are calculated on both the member and full data set level. VSAM key sequenced and relative record data sets, and concatenations with tape data sets, are not supported. This option is only supported for `FOCUS=AUDIT*`.

CHECK=DSN

The syntax for this parameter is `CHECK=({DSN|DSNPREF}=` *`dsn`*`[,DSORG=(PO|PS|VS)])`.

Use this parameter to request checksum (*fingerprint*) computation for data sets. This is sometimes called *freezing*. All data sets specified using the DSN or DSNPREF values are checked to see whether they have a matching DSORG (an omitted DSORG is equivalent to DSORG=(PO,PS,VS)). If so, they are read and two checksum computations are performed: one for global comparison, and one for change control audit or and virus detection. (The latter requires a user-specific CHECKPWD parameter.) For PDS(E) data sets selected with this method, checksums are calculated on both the member and full data set level. VSAM key sequenced and relative record data sets are not supported. The CHECK parameter is allowed under FOCUS=AUDIT*. Also see “Specifying alternate data sources” on page 1597.

CHECK=NO

Specify *NO* to deactivate checking (see CHECK=YES). This value is implied if zSecure Admin, Alert, Tivoli Compliance Insight Manager or Tivoli Security Information and Event Manager are active (FOCUS=ADMINRACF, ALERT*, TCIM*, and VISUAL, if no other focuses are present. The `CHECK=NO` setting is also the default for the AUDIT* focus.

CHECK=YES
Use this parameter to request checksum (*fingerprint*) computation at the member and data set level for partitioned data sets. This is sometimes called *freezing*. All partitioned data sets selected by the PDS, PDSDIR, and CHECKDSN parameters are read, and two checksum computations are performed: a *module level signature* for global comparison and another for change control audit or virus detection. The second computation is only performed when a value has been specified for the `CHECKPWD` parameter.

If `CHECK=YES` is specified, the `IDR` processing parameter for collecting load module identification for each member of a partitioned RECFM=U data set has no effect. In addition, scanning for the members is not activated unless SCAN=N is also specified. This is only supported for `FOCUS=AUDIT*`, but even then the default is CHECK=N.

CHECKDSN=
You can use any of the following syntax patterns for this command:

```
CHECKDSN= dsn
CHECKDSN=dsn/vol
```

Use this parameter if you want checksums to be computed at the member and data set level for the specified partitioned data set. Sequential data sets are *not* supported. This parameter can be combined with VTOC=N,PDS=N to make a `CKFREEZE` file that contains no data set information except the specified `CHECKDSN` data sets. Use the CHECK=Y parameter to request checksums for all APF libraries, LPA list data sets, LNKLST concatenation data sets, and JES2 and MSTR procedure libraries. It is *only* supported for FOCUS=AUDIT*. Also see "Specifying alternate data sources" on page 1597.

CHECKPWD=
You can use any of the following syntax patterns for this command:

```
CHECKPWD='txt'
CHECKPWD='txt'
CHECKPWD=word
```

The password has a length limit of 255. The `CHECKPWD=pwd` statement must fit in one line. If `CHECKPWD` is not specified, the site-specific identification string from the CKRSITE module is used.

To provide virus detection capabilities, specify the `CHECKPWD` parameter in combination with the `CHECK=Y` parameter. The password is used to influence the outcome of each member and data set *change detection* checksum (the actual means are non-disclosed).

The `CHECKPWD` parameter does not affect the *module level signature* checksum calculated for global comparison which is the same across multiple users and customers. Specifying different `CHECKPWD` parameters for different users prevents a virus from using the *module level signature* checksum value calculated when `CHECK=Y` for multiple users. To secure the `CHECKPWD` value so it is only accessible to authorized users, make sure that the invocation JCL is read-protected.

CICS

Use the CICS parameter to indicate whether CICS information is to be collected.

CICS=NO
Specify NO to suppress collection of all CICS transaction, program, library and security-related resource information.

CICS=YES
Specify YES to enable the collection of CICS transaction, program, library and security-related resource information.

Use of this option requires APF authorization and the use of cross-memory services. CICS data is not collected if the NOXMEM parameter is specified.

This option is implied by FOCUS=ADMINRACF, AUDIT*, ALERT*, and VISUAL. The option is supported for these focuses only. The following collection rules apply:

- If the FOCUS parameter values ADMINRACF, ALERT*, or VISUAL only are active, collection is restricted to security-related resource information.
- If at least one AUDIT* FOCUS parameter value is active, additional CICS information is collected.

CKFREEZE

You can use any of the following syntax specifications for this command:

```
CKFREEZE=['dsn'|'dsn(mem)'| dsn | dsn(mem)| pathname]
IOCONFIG=['dsn'| 'dsn(mem)'| dsn | dsn(mem) | pathname]
```

Use this parameter to indicate which data set name to allocate the `CKFREEZE` ddname or UNIX file to. The allocation is done with `DISP=SHR`. This specification replaces any current allocation to ddname `CKFREEZE`.

DASD

Use this parameter to manage the allocation behavior of the DASD devices in your system.

DASD=NO
Specify *NO* to prevent allocation of the DASD devices in your system except for reading special data sets. If no other parameters are specified, this setting results in collecting only the configuration information that can be found in the OS control blocks and that can be found by doing I/O to `TAPE` and `SWCH` devices. This includes all device numbers and volume names, but not the physical ids necessary to map (shared) DASD, nor the contents of any VTOC, VVDS, catalog, or PDS. The difference with `ALLOC=N` is that data set contents can still be requested or implied through additional parameters such as `PDS=Y`.

DASD=YES
Specify *YES* (behind an IF command, for example) to negate the meaning of a previous `DASD=NO` statement.

DB2

Use the DB2 parameter to indicate whether DB2 information is to be collected.

DB2=NO
Specify NO to suppress the collection of DB2 region and security-related resource information.

DB2=YES
Specify YES to enable the collection of DB2 region and security-related resource information.

Use of this option requires APF authorization. Some DB2 data is not collected if the NOXMEM parameter is specified.

DEBUG parameters

Use these parameters to manage debugging behavior.

DEBUG

Use this parameter to print debugging information. The INFO parameter must also be specified. Use this parameter only at the request of IBM software support.

DEBUGHANGTEST

The syntax for this parameter is DEBUGHANGTEST= *n*

Use this parameter to specify the program location for the DEBUGHANGVOLUME test. Currently defined locations are 1 (VTOC sense), 2 (VTOC index), 3 (VTOC data), 4 (VSAM by EXCP), 5 (VSAM by VSAM), 6 (between SVC99 and VTOC OPEN). The default is 1. Use this parameter only at the request of IBM software support.

DEBUGHANGVOLUME

The syntax for this command is DEBUGHANGVOLUME= *volume*.

This value identifies on which volume to issue a long wait. In combination with the HWRESERVE parameter, this option causes other systems that need this volume to issue START PENDING messages. Use this parameter to help debug a problem only at the request of IBM software support.

DMS

Use the DMS parameters to determine whether information from the active DMSFILES and AUTHLIB data sets is collected and to specify specific files for collection.

DMS=NO

Specify *NO* to suppress the data collection. This value is implied by FOCUS=ALERT* and TCIM* if no other focuses are present.

DMS=YES

Specify *YES* to request collection of the DSNINDEX and RACFENCD information in the DMSFILES data set of the active DMS as defined in the LNKLST concatenation or STEPLIB. In addition, if DMS PARMLIB security is active, the list of authorized parameter libraries is read from the authorized library (AUTHLIB) member defined by the active DMS. This option is implied by FOCUS=ADMINRACF, AUDIT*, and VISUAL. The option is *only* supported for these focuses. If running under RACF with an AUDIT* focus but without APF authorization, the program only opens the DMSFILES data set automatically if the user has READ authority to it.

DMSFILES=

You can use either of the following syntax patterns to specify this parameter.

```
DMSFILES= dsn
 DMSFILES=dsn/vol
```

Specify this parameter to include the contents of the specified DMSFILES data set in the CKFREEZE file. It is *only* supported for FOCUS=ADMINRACF, AUDIT*, and VISUAL. Also see “Specifying alternate data sources” on page 1597.

DMSPARMS=

You can use either of the following syntax patterns to specify this parameter.

```
DMSPARMS=dsn
 DMSPARMS=dsn/vol
```

Specify this parameter to include the contents of the specified DMSPARMS data set member SYSPARMS in the CKFREEZE file. It is *only* supported for FOCUS=ADMINRACF, AUDIT*, and VISUAL. Also see "Specifying alternate data sources" on page 1597.

DMSUNL=

You can use either of the following syntax patterns to specify this parameter.

```
DMSUNL= dsn
 DMSUNL=dsn/vol
```

Specify this parameter to include the contents of the specified DMSFILES unload in the CKFREEZE file. It is *only* supported for FOCUS=ADMINRACF, AUDIT*, and VISUAL. Also see "Specifying alternate data sources" on page 1597.

ENQ

Use this parameter if you want CKFCOLL to request collection of information from data sets that are exclusively allocated to another user. There is no guarantee that the collection process is completed. To use this parameter, specify ENQ=NO.

ERRDD

Use this parameter to redirect the SYSTERM output to a user-specified *ddname*. This parameter can only be used as a calling parameter in the PARM keyword in JCL. It cannot be used as a command in the input file.

You can use the following syntax to specify this parameter.

```
ERRDD=ddname
```

EXCLUDE

You can use either of the following syntax patterns for this command.

```
EXCL= list
 EXCLUDE= list
```

The EXCLUDE command. See "Selecting data by device or volume" on page 1599.

EXIT

You can specify this command using any of the following syntax patterns:

```
EXIT
 EXIT=([RC=rc],[NOCLEAR|CLEAR])
```

Use the EXIT keyword to stop zSecure Collect after only reading its input. No processing other than syntax verification is done. *rc* is the return code with which zSecure Collect ends. This can be any number in the range 0...99. It is 12 by default. The NOCLEAR value can be specified to indicate that the CKFREEZE file that would have been written by this zSecure Collect run should be left intact so that other processes that depend on its presence do not fail. The default value, CLEAR, indicates that CKFREEZE file is cleared so that it only contains the messages written by the syntax verification process. Using the CLEAR option ensure that no reports are generated with an outdated CKFREEZE file as input. The RC and (NO)CLEAR values are not inherited from previous EXIT statements. When multiple EXIT statements are encountered, the last statement is used with the RC and (NO)CLEAR values that are specified on that statement. If RC and (NO)CLEAR are not specified in the statement, the default values are used.

FOCUS

Use any of the following syntax patterns to specify this command:

```
FOCUS= focus
F=focus
 FOCUS=list
  F=list
```

Use this parameter to specify the intended use of the configuration data. You can specify any of the following values: ADMINRACF, AUDITACF2, AUDITRACF, AUDITTSS, VISUAL, ALERTACF2, ALERTRACF, TCIMACF2, TCIMCICS, TCIMDB2, TCIMRACF, or TCIMTSS. This parameter automatically sets the proper combination of data collection options for the IBM Security zSecure Admin, zSecure Audit for ACF2 (for ACF2, RACF, or Top Secret), zSecure Visual, zSecure Alert (for ACF2 or RACF), and Tivoli Compliance Insight Manager Enabler for z/OS for z/OS (for ACF2, CICS, DB2, RACF, or Top Secret) products, respectively.

Instead of one focus, a list of focuses can be specified enclosed in parentheses. Alternately, you can specify the value ALL or LICENSED to request all focuses recognized by zSecure Collect, which is equivalent to omitting the FOCUS keyword. Also see "Selecting the products for the collect operation" on page 1595.

FREE

Use this parameter to free the files used dynamically as soon as processing has finished. Setting this option makes processing much slower than it is if the default setting is used where all files that are used are freed at one time remain allocated until step termination. If this parameter is not specified, the program starts freeing individual files when it estimates there is space in the TIOT for less than 10 additional ddnames. See message CKF297I at the end of the SYSPRINT for information about actual numbers being freed.

FREEZEDD

Use the FREEZEDD statement to specify the ddname to be used for the CKFREEZE data set.

Use the following syntax to specify this command:

```
FREEZEDD=ddname
```

The specified ddname is used to replace the default CKFREEZE value. The ddname is also used to allocate the data set that have specified on the CKFREEZE statement, if it has not been allocated.

HFS parameters

The following HFS parameters are equivalent to the corresponding UNIX parameters. For details, see "UNIX parameters" on page 1633.

Table 645. HFS parameters

HFS parameter	Equivalent Unix parameter
HFS=YES	UNIX=YES
HSF=NO	UNIX=NO
HFSCLIENT=YES	UNIXCLIENT=YES
HSFCLIENT=NO	UNIXCLIENT=NO

HSM parameters

Use the HSM parameters to control collection of HSM Backup and Migration data.

HSMBCD=

Use either of the following syntax patterns for this command:

```
HSMBCD= dsn
  HSMBCDS=dsn/vol
```

Use this parameter to include the contents of the specified HSM Backup Control data set in the CKFREEZE file. This option is *only* supported for FOCUS=ADMINRACF, AUDIT*, and VISUAL. Also see "Specifying alternate data sources" on page 1597.

HSMMCD=

Use either of the following syntax patterns for this command:

```
HSMMCD= dsn
 HSMMCDS=dsn/vol
```

Use this parameter to include the contents of the specified HSM Migration Control data set in the CKFREEZE file. This option is *only* supported for FOCUS=ADMINRACF, , AUDIT*, and VISUAL. Also see "Specifying alternate data sources" on page 1597.

HWRESERVES (no longer valid)

This parameter is no longer valid.

ICFCAT

Use either of the following syntax patterns for this command:

```
ICFCAT= dsn
ICFCAT=dsn/vol
```

Use this parameter to request that the catalog contents of the specified ICF catalog be included in the CKFREEZE file. Also, see "Specifying alternate data sources" on page 1597.

IDR

Use this parameter to control the collection of load module identification for each member of a partitioned RECFM=U data set.

IDR=NO

Specify *NO* (behind an IF command, for example) to negate the meaning of a previous IDR=YES statement or default. NO is the default, unless CHECK=YES is also specified. If that option setting is specified IDR=YES is the default value.

IDR=YES

Specify *YES* to request extraction of the load module identification information If you specify this setting, all partitioned data sets selected by the PDS, PDSDIR, and CHECKDSN parameters are read. The information consists of link-edit date, any ZAP information, and unique IDR strings (usually PTF numbers) with the most recent date that accompanies each string. The IDR=YES setting is supported *only* for FOCUS=AUDIT*, but even then the default is IDR=N. IDR=Y is implied by CHECK=Y.

IF

Use any of the following syntax patterns for this command.

```
IF symbol = list :
IF symbol <> list
```

Use this keyword to skip or include a line of parameters, based on the SMFID of the system or a Static System Symbol. You can specify the following variables with this keyword.

symbol
Specify any symbol in the Static System Symbol table without the preceding ampersand or ending period or the SMFID. If the symbol cannot be found in the Static System Symbol table, this field is considered empty and only matches an empty string.

list
Either a single value or a list of comma-separated values, enclosed in parentheses. Each value can be enclosed in double or single quotation marks. Values specified without quotation marks are converted to uppercase. If a value is an empty string or contains lowercase characters, non-alphanumeric characters, or national characters, you must enclose the value in quotation marks. Trailing blanks in either the symbol or the value are ignored.

When the test specified in the IF statement evaluates to false, the rest of the line is skipped which means that no syntax checking occurs. If the test evaluates to true, the rest of the line is parsed normally. Do not put the IF statement itself at the start of a line. IF statements can be nested, but no end-of-line is permitted between the IF and the colon (:) marking the end of the test condition. A blank is required after the colon.

IMS

Use the IMS parameter to indicate whether IMS information is to be collected.

IMS=NO
Specify NO to suppress the collection of IMS transaction, PSB and security-related resource information.

IMS=YES
Specify YES to enable the collection of IMS transaction, PSB and security-related resource information.

Use of this option requires APF authorization. Some IMS data is not collected if the NOXMEM parameter is specified.

This option is implied by FOCUS=ADMINRACF, AUDIT*, ALERT*, and VISUAL. The option is supported for these focuses only. The following collection rules apply:

- If the FOCUS parameter values ADMINRACF, ALERT*, or VISUAL only are active, collection is restricted to security-related resource information.
- If at least one AUDIT* FOCUS parameter value is active, additional IMS information is collected.

INDD

Use this parameter to redirect SYSIN to a user-specified data set *ddname* so that SYSIN is read from the specified ddname. This parameter can only be used as a calling parameter in the PARM keyword in JCL. It cannot be used as a command in the input file.

You can use the following syntax to specify this parameter.

```
INDD=ddname
```

INFO

Use this parameter to obtain information about the progress of processing. The information is not presented in a structured way, but it can be used to get an insight in the amount of parallelism. The INFO parameter is mainly intended for debugging and analyzing zSecure Collect performance.

INTERVAL (no longer valid)

This parameter is no longer valid.

IO parameters

Use the IO command to specify whether solicited I/O to devices is permitted and to specify a timeout value.

IO=NO

Specify *NO* to prevent any solicited I/O to devices. This setting implies ALLOC=N, DASD=N, PDS=N, MCD=N, BCD=N, CAT=N, TMC=N, DMS=N, RMM=N, VMF=N,UNIX=N, ABR=N, TAPE=N, SWCH=N. (That is, these parameters cannot be set to Y.) If no other parameters are specified, it results in collecting only the configuration information that can be found in the OS control blocks. This includes all device numbers and volume names, but not the physical ids necessary to map (shared) DASD tapes, and switches, nor the contents of any VTOC, VVDS, catalog, UNIX file system, or PDS. Explicitly requesting special data sets by data set name does *not* result in I/O (this is the difference with UNITIO=N).

IO=YES

Specify YES to negate the meaning of a previous IO=NO statement, behind an IF command for example.

IOTIMEOUT

The syntax for this parameter is IOTIMEOUT= *nnn*.

Use this parameter to change the default timeout period for the Missing Interrupt Handler, or to deactivate it. The default value is *60* seconds. To deactivate the timeout mechanism, set this value to *0*. When the mechanism is deactivated, the Missing Interrupt Handler shows START PENDING messages on the console if it misses an interrupt. The IOTIMEOUT parameter prevents the program from hanging on a long reserve if the program runs with APF authorization and SIO=YES. This setting does not necessarily prevent hanging if the long reserve starts while the program is already doing I/O to the device. The I/O timeout feature only works on z/OS release 1.2 and higher.

LICENSE (no longer used)

This parameter is no longer used.

MCD

Use this parameter to determine whether information is collected from the active HSM Migration Control Data set.

MCD=NO

Specify *NO* if you do not want to collect information from the active HSM Migration Control Data set. This setting is implied by FOCUS=ALERT*, and TCIM* if no other focuses are present.

MCD=YES

Specify *YES* to request collection of the information from the Migration Control Data set of the active HSM. This setting is implied by FOCUS=ADMINRACF, AUDIT*, and VISUAL and is *only* supported for these focuses. This setting is only honored if the program is running APF-authorized, because APF authorization is needed to determine the data set name. Also, the HSM address space must be swapped in to do this automatically.

MOD

Use this parameter to control the collection of load module and exit information. This includes SVC and PC routines. RACF and ACF2 exit information will always be collected regardless of the setting.

MOD=NO
Specify NO to not collect module information.

MOD=YES (default)
Specify YES to collect all load modules, SVC and PC routines, and exit information.

MONITOR (no longer valid)

This parameter is no longer valid.

NJE

Use this parameter to control the collection of JES node information.

NJE=NO
Specify NO to not collect JES node information.

NJE=YES (default)
Specify YES to collect JES node information.

NOBSAMBPAM

This parameter is valid on the `PARM` string only. Use this setting to disable use of the BSAM and BPAM access methods by the program. The program uses QSAM instead. Use this parameter only at the request of IBM software support.

NOBYPASS

Use this APF-only parameter to prevent bypassing data set security for dumping ICF and HSM catalogs, PDS directories, and DMS, ABR, CA1, TLMS, and RMM data sets. Use this parameter only at the request of IBM software support.

NOCLOSE

Use this parameter to leave files open at abnormal termination of the program to be able to debug problems. It can only be used in the parameter string, not in the SYSIN file. Use this parameter only at the request of IBM software support.

NODCBE

Use this parameter if you do not want to use buffers above 16 MB for certain input files. This option can only be used in the parameter string, not in the SYSIN file. Use this parameter at the request of IBM software support.

NODIAG

Use this APF-only option to prevent use of the `DIAGNOSE` instruction to issue VM queries if MVS is running under VM. This option causes VM-specific data to be missing. It can also cause command rejects on 3990 devices (message IOS000I) because VM blocks certain query CCWs. Use this parameter only at the request of IBM software support.

NOKEY0

Use this APF-only option to prevent use of the APF-authorized access to fetch protected control blocks (like the PPT and TCAST). This causes the fetch protected information to be missing. Use this parameter only at the request of IBM software support.

NOMSG

The syntax for this parameter is `NOMSG= list`

This option is equivalent to the SUPMSG. See "SUPPRESS" on page 1631.

NOREPORT

Use this option to suppress the volume, PDS, special data set, and catalog reports.

NOSIO

This APF-only option can be set to prevent use of the APF-authorized I/O driver. This causes fallback to non-authorized ways of finding paths for DASD devices. No path information is found for tape devices. No cache size and caching status information is collected for 3880 model 23 devices. Use this parameter only at the request of IBM software support.

NOUID0

This APF-only option can be used to prevent the use of APF authorization to switch to UNIX UID 0 in order to scan all file system directories. If this option is specified, file system access is done under the UID for the user, which might cause a failure to read some directories. Use this parameter only at the request of IBM software support.

NOXMDSN

This APF-only option can be set to prevent collecting data set names and types by means of cross memory instructions (a subset of cross memory operation). Use this parameter only at the request of IBM software support.

NOXMEM

This APF-only option can be set to prevent the use of any cross-memory instructions. It results in missing information about PC/AUTH, RMF, HSM, RMM, and JES2. Use this parameter only at the request of IBM software support.

OFFLINE

The syntax for this parameter is `OFFLINE=YES`.

Use this parameter to include UCB type information for offline devices.

OUTDD

Use this parameter to redirect the `SYSPRINT` output to a user-specified *ddname*. This parameter can only be used as a calling parameter in the PARM keyword in JCL. It cannot be used as a command in the input file.

You can use the following syntax to specify this parameter.

```
OUTDD=ddname
```

PARALLEL

Use either of the following syntax patterns for this command:

```
PARALLEL= option
 PAR=option
```

Use this parameter to select the amount of parallelism, and hence the amount of storage used by zSecure Collect. When you specify `PARALLEL`, the *option* variable can have any of the following values.

Table 646. CKFCOLL PARALLEL parameter - available option values

Option	Description
NONE	Forces sequential operation, that is to access only one device at a time.
PATHGROUP	Requests a maximum of one I/O per group of paths (and hence per LCU). Use this value if there is insufficient storage available for the default, or if PATH adds too much I/O to a heavily loaded LCU.
PATH	PATH is the default setting. This setting indicates that I/O is scheduled for at most one device per channel path.

PATH

Use this parameter to determine processing behavior for all paths to a device.

PATH=YES

Specify *YES* to include processing to obtain information across all paths to a device.

PATH=NO

Specify *NO* to suppress processing to obtain information across all paths to a device. This value is the default setting.

PDS

Use the PDS parameters to control the behavior of PDS directory dumps and determine the type of data to be included in the dumps.

PDS=

Use the PDS parameter to determine whether the PDS directory is dumped.

PDS=NO

Specify *NO* to suppress PDS directory dumps. This setting is the default if the program is not running APF-authorized. This value was chosen as the default to prevent a large number of 913-38 abends.

PDS=YES

Specify *YES* to cause collection of PDS and PDS/E directories of APF, LNKLST concatenation, and LPA list data sets as well as JES2 and MSTR procedure libraries, IEFJOBS, and SYS1.UADS (the latter only with FOCUS=AUDIT*). This setting is implied if the program is running under RACF or running APF-authorized. Keep the following processing considerations in mind when using this parameter with the CKFCOLL program.

- If the program is not running APF-authorized or under RACF with an AUDIT* focus, the PDS=YES parameter must be specified explicitly.
- If the program is not running APF-authorized or under RACF with an AUDIT* focus, READ access is required to all PDSs to be accessed.
- If the program is not running APF-authorized but is under RACF with an AUDIT* focus, the program only accesses partitioned data sets automatically if the user has READ authority to.

PDSDIR=

Use either of the following syntax patterns for this command.

```
PDSDIR= dsn
 PDSDIR=dsn/vol
```

Use this parameter to specify that the directory information of the indicated partitioned data set is included in the CKFREEZE file. This option is only permitted for FOCUS=ADMINRACF, ALERT*, AUDIT*, and TCIM*. Also see "Specifying alternate data sources" on page 1597.

PDSEBUFSIZE

The syntax for this command is PDSEBUFSIZE= *nn*.

Use this parameter to set an upper limit to the amount of user IDR data to store per PDSE program object, in kilobytes This parameter is only relevant if IDR=YES has been specified or implied. The *nn* value can be in the range of 1 to 1024, inclusive, and defaults to 128. Because the program typically uses about 10 of these buffers per PDSE, specifying a lower value can significantly reduce storage use.

RECALL

Use this parameter to determine whether the CKFCOLL program tries to recall (HSM) or restore (DMS or ABR) the data sets containing requested information (PDS directories, for example) if they are not found on their volume.

RECALL=NO

Specify *NO* to warn zSecure Collect not to attempt to recall (HSM) or restore (DMS or ABR) the data sets not found on their volume. This setting is the default for FOCUS=VISUAL only. RECALL is a synonym of RESTORE. If RECALL=NO is combined with VTOC=NO, alternate data sources for which no volser is explicitly specified might not be processed. For details, see "Specifying alternate data sources" on page 1597.

RECALL=YES

Specify *YES* (behind an IF command, for example) to negate the meaning of a previous RECALL=NO statement or default. YES is the default value if FOCUS=ADMINRACF, ALERT*, AUDIT*, or TCIM*.

REPORT

Use this parameter to create volume, catalog, and special data set reports. This option is set by default.

RESTORE

Use this parameter to determine whether the CKFCOLL program tries to recall (HSM) or restore (DMS or ABR) the data sets containing requested information (PDS directories, for example) if they are not found on their volume. This parameter is a synonym for the RECALL parameter.

RESTORE=NO

Specify *NO* to warn zSecure Collect not to attempt to recall (HSM) or restore (DMS or ABR) the data sets not found on their volume. This setting is the default for FOCUS=VISUAL only. RECALL is a synonym of RESTORE. If RESTORE=NO is combined with VTOC=NO, alternate data sources for which no volser is explicitly specified might not be processed. For details, see "Specifying alternate data sources" on page 1597.

RESTORE=YES

Specify *YES* (behind an IF command, for example) to negate the meaning of a previous RESTORE=NO statement or default. YES is the default value if FOCUS=ADMINRACF, ALERT*, AUDIT*, or TCIM*.

RMM

Use this parameter to control whether CKFCOLL collects information from the active RMM control data set. It is implied by FOCUS=ALERT*, TCIM*, and VISUAL if no other focuses are present.

RMM=NO
Specify *NO* to suppress collection of information from the active RMM control data set. this setting is implied by FOCUS=ALERT*, TCIM*, and VISUAL if no other focuses are present.

RMM=YES
Specify *YES* to cause collection of RMM volume, data set, and ownership records from the Removable Media Manager (RMM) control data set of the active RMM system as defined by storage control blocks. This option is implied by FOCUS=ADMINRACF and AUDIT*, and is *only* supported for these focuses.

RMMCTL

This command can be specified using either of the following statements:

RMMCTL= *dsn*
RMMCTL=*dsn/vol*

command is PDSEBUFSIZE= *nn*.

Request to include the tape data set, volume, and owner data from the specified Removable Media Manager Control data set in the CKFREEZE file. It is *only* supported for FOCUS=ADMINRACF and AUDIT*. Also see "Specifying alternate data sources" on page 1597.

SCAN

Use this parameter to control scanning operation of in-core modules and PDS members selected for checking using the CHECK and CHECKDSN parameters.

SCAN=NO
Specify *NO* to deactivate scanning. This value is implied if no AUDIT* focuses are present.

SCAN=YES
Specify YES to activate scanning of in-core modules selected for eye catcher processing, as well as PDS members selected for checking (by means of the CHECK and CHECKDSN parameters). Scanning is performed for dangerous functions that warrant auditing of the module and for the strings implied by the SCANSVC and SCANSTR parameters. This value is implied by FOCUS=AUDIT*, and is *only* supported under these focuses.

SCANSTR= *list*
Use this parameter to specify a text string, or a list of text strings enclosed in parentheses and separated by commas to be used for scanning. In-core modules like SVCs and exits, as well as PDS members are scanned for the text strings (PDS members only if CHECK=Y or CHECKDSN= has been specified). Only the first 7 strings in the list are reported separately per member in the CKFREEZE file. Hits in the remaining set of strings are combined into one yes/no flag. A text string can be a word (without quotation marks, blanks, or separators), a string enclosed in single quotation marks (without single quotation marks in the string), or a string enclosed in double quotation marks (without double quotation marks in the string). The length is limited to 255 bytes and each text string in the list must fit in one line. For FOCUS=AUDIT*, a scan argument is automatically added to search for a specific published security exposure in a third-party product.

SCANSVC= *list*
Use this parameter to specify either one SVC number in decimal or a list of SVC numbers (decimal) enclosed in parentheses and separated by commas to be used for scanning. In-core modules like SVCs and exits, as well as PDS members on DASD are scanned for SVC instructions invoking the specified SVCs. PDS members are scanned only if CHECK=Y or CHECKDSN= has been specified. Only the first 7 numbers in the list are reported separately per member in the CKFREEZE file; hits in the remaining set of SVCs calls are combined into one yes/no flag.

SELECT

You can specify this command using any of the following statements:

```
SELECT= list
SEL= list
S=list
```

syntax for this command is `S = list.`

The SELECT command. See "Selecting data by device or volume" on page 1599.

SERIALIZATION

The syntax for this command is `SERIALIZATION=( serialization-options).`

Use this option to specify which measures the program takes to ensure data integrity for the CKFREEZE data set. For serialization to operate properly, all jobs involved need to use the same resource name. That is, all jobs must specify the same ENQ option. All jobs should furthermore access data sets under their true names. Do not use aliases because a successfully acquired alias does not guarantee that the data set is available under its true name. The serialization options that can be specified are:

ENQ=(*qnames***)**
Serialization option for ensuring data integrity and input data availability by specifying that the program issue the appropriate ENQ request. You can specify the following subparameters to indicate the desired type of processing:

CKRDSN
The program issues a sysplex-wide exclusive ENQ with the specified QNAME for the CKFREEZE data set that it writes to. This way, it is guaranteed that no other process attempts to read the CKFREEZE while the system refreshes it.

SYSDSN
The program issues a system-wide shared ENQ with this QNAME for the CKFREEZE data set it writes to. This ENQ is intended to be used in combination with the WAIT serialization option, so that the program can wait until the required data set is available. Alternatively, when used in combination with the FAIL serialization option, an error message is issued if the data set is not immediately available, and further processing is ended. Issuing an ENQ request for QNAME SYSDSN requires that the program be APF authorized.

This option is mutually exclusive with NOENQ.

FAIL
This serialization option specifies that the program is to abort further processing if the CKFREEZE data set for which an ENQ is requested is not immediately available. This option is mutually exclusive with WAIT. If neither is specified, FAIL is the default.

MAXWAIT(*nn*)
This serialization option specifies the maximum time the program should wait for the CKFREEZE data set for which an ENQ is requested to become available, in minutes. Supported values are 1 - 59, inclusive, with a default value of 5 minutes. This option only has an effect in conjunction with serialization option WAIT.

NOENQ
This serialization option specifies that no ENQs are to be issued. This option is mutually exclusive with ENQ.

UNIT
This serialization option specifies that, if need be, dynamic allocation waits until a unit becomes available to satisfy the allocation request. It applies mostly to tape data sets. This option requires that the program be APF authorized.

VOLSER
This serialization option specifies that, if need be, dynamic allocation waits until the required volser becomes available. It applies mostly to tape data sets. This option requires that the program be APF authorized.

WAIT
This serialization option specifies that the program is to wait until the CKFREEZE data set for which an ENQ is requested is available. This option is mutually exclusive with FAIL. If the program is APF authorized, you can use the MAXWAIT serialization option to specify a maximum wait time. An unauthorized program can only wait until the CKFREEZE data set is available.

By default, the program uses the settings SERIALIZATION(ENQ(CKRDSN),FAIL. Any errors encountered during input parsing cause the program to revert to these default settings.

SHARED

Determines how information from shared disk devices is processed.

SHARED=NO

Specify NO to turn off processing for information from shared disk devices, unless system-specific. When this option is selected, no records are written for VTOC, VVDS, user catalog, migration, backup, or tape catalog information for volumes generated as *shared*. Although records are not written, the VTOC and VVDS are still read–not dumped–to scan for data sets of importance. In addition, the PDS directories selected or implied are all dumped, as is the master catalog.

Use this parameter when you want to reduce processing time in (partially) shared DASD configurations. This can be accomplished by running zSecure Collect without specifying SHARED=NO on one system and specifying SHARED=NO on the other systems. ***Note***: If the zSecure Collect FOCUS parameter specifies ADMINRACF, AUDIT*, and TCIM*, setting SHARED=NO might result in missing migration catalog or user catalog information if these catalogs are different among the systems that are sharing the volumes, and the catalogs do not reside on a non-shared volume.

SHARED=YES

Specify SHARED=YES to negate the effect of a previousSHARED=NO statement. For example, if you have specified SHARED=NO but want to enable information processing of information from shared volumes under some conditions, you can specify SHARED=YES within an IF statement. *YES* is the default value for the SHARED keyword.

SIGVER

This parameter determines whether signature verification information is to be collected when collecting directory information from a PDSE (partitioned data set extended).

SIGVER=NO
When SIGVER=NO is specified zSecure Collect does not collect signature verification information. This is the default value for this parameter.

SIGVER=YES
When the signature verification service is available on a z/OS system, use the SIGVER=YES parameter setting to enable the collection of signature verification information when collecting directory information from a PDSE (partitioned data set extended). If the signature verification service is not available message CKF362I is issued and the job terminated.

Signature verification is not done if the following zSecure Collect parameter values are specified: DASD=N or PDS=N.

SLOWDOWN

Use this option to force the use of VSAM OPEN and GET commands to read all catalogs. Its main use is to maintain operation in a pre-DFP V3 system without APF authorization, but with ALTER permits on the catalogs.

SMS=NO

Use this parameter to suppress SMS calls to obtain information about all structures except storage groups. This can save some elapsed time if you do not need SMS construct data. The default is to read SMS construct data for all focuses.

STATS (no longer valid)

This parameter is no longer used.

STORAGEGC

Use this parameter to turn on garbage collection during the run. In some cases this reduces storage consumption, but CPU usage increases. It can only be used in the parameter string, not in the SYSIN file.

SUPPRESS

This command can be specified using any of the following syntax:

```
SUPMSG=list
SUPP=list
SUPPMSG=list
  SUPPRESS=list
```

Use this command to suppress all messages with the specified number or numbers. You can specify one decimal number, or a list of numbers enclosed in parentheses and separated by commas. For instance, SUP=17 suppresses 'path not operational' messages that are to be expected in an LPAR system.

SWCH (no longer valid)

This parameter is no longer valid.

TAPE (no longer valid)

The TAPE parameter is no longer used.

TCPIP

Use this parameter to control the collection of TCP/IP stack configuration data and CS Resolver configuration data. In order to collect this data, CKFCOLL must run APF-authorized.

TCPIP=NO
Specify *NO* to turn off collection of TCP/IP stack configuration data and CS Resolver configuration data from the Communications Server.

TCPIP=YES
Specify *YES* to enable the collection of TCP/IP stack configuration data and CS Resolver configuration data. The value `TCPIP=YES` is authorized with an entitlement for the following products: `AUDITACF2`, `AUDITRACF`, `AUDITTSS`, `ALERTACF2`, or `ALERTRACF`. TCPIP=YES is the default value for systems with the correct entitlement.

TMC

Use this parameter to determine whether active CA1 Tape Management Catalog is collected.

TMC=NO
Specify *NO* to suppress data collection from the active CA1 Tape Management Catalog. This value is implied by `FOCUS=ALERT*`, `TCIM*`, and `VISUAL` if no other focuses are present.

TMC=YES
Specify *YES* to cause collection of TMC volume records and DSNB records from the Tape Management Catalog (TMC) of the active CA1 as defined by an MVS subsystem. This option is implied by `FOCUS=ADMINRACF` and `AUDIT*`, and is *only* supported by these products. If running under RACF with an `AUDIT*` focus but not APF authorized, the program only opens the tape catalog automatically if the user has READ authority to it.

TMCDSN

This command can be specified using any of the following syntax:
`TMCDSN= dsn`
`TMCDSN=dsn/vol`

Request to include the tape catalog contents of the specified UCC1 or CA1 Tape Management Catalog in the `CKFREEZE` file. It is *only* supported for the entitlements `FOCUS=ADMINRACF` and `AUDIT*`. Also see "Specifying alternate data sources" on page 1597.

UNCONNECTED

Use this APF-only option to set unconnected catalogs for dumping. The main use for this option is during volume selections that exclude the master catalog volume. `OPEN` for unconnected catalogs requires either APF authorization or inclusion of a `STEPCAT` or `JOBCAT` ddname for the unconnected catalog.

UNITIO

Use this parameter to control behavior of I/O to devices.

UNITIO=NO
Specify *NO* to only authorize explicitly solicited I/O to devices. This setting implies the following CKFCOLL parameter settings: `ALLOC=N`, `DASD=N`, `PDS=N`, `MCD=N`, `BCD=N`, `CAT=N`, `TMC=N`, `DMS=N`, `RMM=N`, `VMF=N`, `UNIX=N`, `ABR=N`, `TAPE=N`, and `SWCH=N`. (That is, these parameters cannot be set to `Y` unless `UNITIO` itself is overridden). This does not prevent I/O to explicitly requested data set names. The `CKFREEZE` file includes all device numbers and volume names, but not the

physical ids necessary to map (shared) DASD tapes, and switches, nor the contents of any VTOC, VVDS, catalog, UNIX file system, PDS, or tape/DASD management catalog unless requested by data set name.

UNITIO=YES
Specify *YES* (behind an IF command, for example) to negate the meaning of a previous `UNITIO=NO` statement.

UNIX parameters

Use these parameters to whether UNIX file directory data is collected and to specify the type of data collected.

UNIX =

UNIX=NO
Specify *NO* to suppress collection of z/OS UNIX file directory data. This setting is implied by `VISUAL` if no other focus is present.

UNIX=YES
Specify *YES* to request collection of the z/OS UNIX file directory data from the Hierarchical File System of the current system. This setting is implied by `FOCUS=ADMINRACF`, `FOCUS=ALERT*`, `AUDIT*`, and `TCIM*` and is only supported by these products. If you specify this setting, data collection takes a considerable amount of time. Running APF ensures that all directories can be dumped and makes the process run faster. Also see `UNIXCLIENT` and `AUTOMOUNT`. The userid running CKFCOLL must have an OMVS segment; otherwise the message `CKF320I` with system abend EC6 is issued, or message ICH408I if the default UNIX user exists and is revoked.

UNIXACL=
Use this command to determine whether UNIX ACL entry data is collected.

UNIXACL=NO

Specify *NO* to suppress collection of `UNIX ACL` entries. This value is implied by `UNIX=NO`.

UNIXACL=YES
Specify *YES* to request collection of all UNIX ACL entries. This setting is only honored if `UNIX=YES` is specified or implied, too. This value is implied by `UNIX=YES`.

UNIXCLIENT
Use this parameter to determine whether z/OS UNIX file directory data is collected from the UNIX File System of other systems that are connected through XCF. Generally, you can run CKFCOLL on each system separately which results in a dump of the UNIX File System for each system. Using this method, you do not have to run CKFCOLL through the network to the client, which takes much longer than reading directly from the disk. Because of this situation, the default value for this parameter is *NO*.

UNIXCLIENT=NO

Specify *NO* to prevent collection of z/OS UNIX file directory data from the UNIX File System of other systems that are connected through XCF. That is, this parameter says not to dump UNIX data where the UNIX File System is only mounted as a client. This is the default setting for this parameter.

UNIXCLIENT=YES

Specify *YES* to request collection of z/OS UNIX file directory data from the UNIX File System of other systems that are connected through XCF. That is, this parameter requests to dump UNIX data where the UNIX File System is only mounted as a client.

VMF parameters

Use these parameters to determine whether data is collected from the active TLMS volume master file and to specify the type of data to collect.

VMF=

Use this parameter to determine whether the data is collected.

VMF=NO

Specify *NO* to suppress collecting information from the active TLMS volume master file. It is implied by `FOCUS=ALERT*, TCIM*`, and `VISUAL*` if no other focuses are present.

VMF=YES

Specify *YES* to request collection of TLMS control, volume base, volume link, and data set records from the Tape Library Management System (TLMS) volume master file of the active TLMS system as defined by incore control blocks. This option is implied by the entitlements `FOCUS=ADMINRACF` and `AUDIT*`, and is supported only by these products. If running under RACF with an `AUDIT*` focus but not APF authorized, the program only opens the volume master file automatically if the user has `READ` access to it.

VMFDSN

Use this parameter to include the control, volume base, volume link, and data set data from the specified Tape Library Management System volume master file in the `CKFREEZE` file. It is only supported for entitlements `FOCUS=ADMINRACF` and `AUDIT*`. Also see "Specifying alternate data sources" on page 1597.

The syntax for this command is
`VMFDSN= dsn`
`VMFDSN=dsn/vol`

VTOC

Use the VTOC parameter to determine whether DSCB, VVR/NVR, and ICF catalog information is collected.

VTOC=NO

Specify *NO* to suppress collection of all DSCB, VVR/NVR, and ICF catalog information. This setting implies `VVDS=N,CAT=N`. If no other parameters are specified, this value results in the complete configuration information with the device as the smallest entity plus the contents of any PDS directories and tape/DASD management catalogs implied by the focus.

VTOC=YES

Specify *YES* to request collection of all DSCB and VVR information. The VTOC tracks that contain used DSCBs are read. `VTOC=YES` is the default setting.

VVDS

Use this parameter to control collection of the VVR and NVR information.

VVDS=NO

Specify *NO* to suppress collection of VVR and NVR information. This value is implied by `VTOC=N`. The VVDS data sets are not allocated and opened unless they are needed to obtain information on a tape/DASD management or ICF catalog. If no other parameters are specified, this results in complete

configuration information with the physical data set extent as the smallest entity, but no information is obtained on the cluster name and nature of VSAM physical components. This can result in non-informational system-generated VSAM names in your reports.

VVDS=NONE

Specify *NONE* to suppress collection of VVR and NVR information. This value is stronger than VVDS=N. The VVDS data sets are never allocated and opened. Its main use is to circumvent errors during VVDS processing.

VVDS=YES

Specify *YES* to request collection of VVR and NVR information. The VVDS data sets are opened and the tracks with used control intervals are read. It is the default.

WAIT=NO

Use this non-APF option to determine whether CKFCOLL collects information about retry waits used in attempts to collect data on all physical paths to a device.

WAIT=NO

Specify *NO* to suppress retry waits. Use this value to speed up operation if you are only interested in device contents layout such as VTOC.

WAIT=YES

Specify *YES* (behind an `IF` command, for example) to negate the meaning of a previous `WAIT=NO` statement.

X=list

This parameter is the `EXCLUDE` command. See "Selecting data by device or volume" on page 1599.

XTIOT

The XTIOT parameter manages the behavior of XTIOT control blocks. This parameter can have the following values.

XTIOT=NO

Block the use of z/OS `XTIOT` control blocks for non-VSAM allocations.

XTIOT=YES

Default. Enables dynamic allocation to indicate that z/OS `XTIOT` control blocks are to be used for relief of file allocation limits and below the line virtual storage constraint relief. This option has two prerequisites: Requires z/OS 1.12 support for the `NON_VSAM_XTIOT` PARMLIB option. Requires that the `NON_VSAM_XTIOT=YES` setting is coded in an active `DEVSUPxx` member of the z/OS PARMLIB. If these prerequisites are not met, then `XTIOT=YES` is silently ignored.

3350 (no longer valid)

This parameter is no longer used.

Troubleshooting

For details on zSecure Collect abends that occur during operation, see "Abends" on page 1636. This section lists common abend codes and explains the actions you can take to correct the problem. For other issues, see "Other Problems" on page 1638.

If zSecure Collect operation stops with abend errors, see "Abends" on page 1636 for information about the errors.

Abends

This topic lists the most common abend codes encountered with zSecure Collect. Each abend description also includes suggestions for possible causes and remedies. You can also check the appropriate message manual for your operating system for the exact meaning of an abend and reason code on your system.

001
Usually indicates problems with block size. Look at the message in your job log to determine the ddname.

002
Problems with the DCB parameters of a file. Look at the message in your job log to determine the ddname. Check your specification for DCB parameters with the reference material in "Calling zSecure Collect using JCL" on page 1603.

113-40
This abend with message IEC142I can occur for the `VVDS` or a `CATINDEX`. If the abend occurs for `VVDS`, you are experiencing a problem identified by IBM APAR OW22180. This problem usually starts after service for IBM APAR OW18440 (RLS toleration PTFs) has been applied. You can work around this problem by re-cataloging the VVDSes that cause an abend. If the abend is issued for the `CATINDEX`, then you are experiencing a problem identified by IBM APAR OW23404, which starts happening after applying service for IBM APAR OW22180 (113-40 fix for VVDSs).

When this abend occurs zSecure Collect continues operation with the next dataset on the volume.

213-04
This abend can occur for the VTOC on online volumes that have not been initialized. It can also occur for APF libraries that are not physically present on the volume. zSecure Collect continues operation with the next volume.

213-20
An abend 213-20 can occur on pre-DFP V3 systems if a catalog has more than 16 extents. zSecure Collect intercepts the abend and enters slowdown mode (for example, use VSAM GET, running much slower on shared DASD systems).

322
CPU time limit exceeded. Check the job log for prior abend messages with a different abend code. If a prior abend occurred, solve this abend. Otherwise, increase the `TIME` parameter on the `JOB` card, code fewer functions together, or split the input, specify input per FOCUS for example. Large sites with FOCUS=ADMINRACF or AUDIT* might require a CPU time limit more than a minute on z990 processors. For other sites, a time limit of a minute is normally sufficient. However, if you have specified `CHECK=YES` or have many UNIX files, a time limit of 10 minutes might be required.

522
In the job log, check that the job was not waiting for a tape mount, offline, inaccessible, or reserved device. In the latter case, you can circumvent problems by excluding the inaccessible volume with an EXCLUDE command.

722
Too many output lines. Make your selection more specific or increase the output limit for your job. For example, with a `/*JOBPARM L=`*nn* card, where *nn* represents thousands of lines permitted).

80A, 878
GETMAIN error. Try to increase the REGION parameter on the EXEC or JOB card. If you have reached the maximum size for your site, code fewer functions together, reduce parallelism–by specifying PARALLEL=PATHGROUP for example, or split the input, per FOCUS or per LCU for example. The variable memory usage is slightly more than 64 kB below the line per I/O executor. For the number of I/O executors allocated, see the output from message CKF111I, which is documented in the *IBM Security zSecure: Messages Guide*.

913-0C
An abend 913-0C occurs if attempting to open an unconnected ICF catalog without bypassing RACF data set security. This problem can occur if a selection is done that excludes the master catalog volume, while specifying CAT=YES. If the catalog is in fact connected, then you might be running into a problem caused by IBM APAR OW22180 that starts happening after applying service for IBM APAR OW18440 (RLS toleration PTFs). If this problem occurs, you must also install the fix for IBM APAR OW23404 because otherwise you only change the abend code from 913-0C to 113-40. zSecure Collect intercepts the abend and continues with the next catalog.

913-38
Abend 913-38 occurs if a PDS or other DMS or CA1 non-VSAM data set is opened but you do not have authorization to do so, either through the DATASET profile or through the resource corresponding to your FOCUS (for example, CKF.AUDIT) when running the program with APF authorization.

B37, D37
One of the output data sets was too small, or there was no space left on the volume to extend the data set. Look at the message in your job log to determine the ddname.

DC2
This diagnostic abend is issued by the IARV64 service, which handles storage above the bar. The reason for the abend is explained by the MVS System Code documentation.

EC6
Abend EC6, indicated by message CKF320I can occur under the following condition: The user running zSecure Collect has specified or implied the UNIX=YES setting, the user ID has no OMVS segment, and no default UNIX user ID exists, or there is a default UNIX user ID but it is revoked, or it does not have an OMVS segment. Other EC6 abends can be caused by anything; the abend code indicates that the problem occurred while in a UNIX service. You must have the reason code to know what caused the problem, which might be something like CPU time limit reached - reason FD1D. See the “abend 322” on page 1636 description for details.

User Abends
Generally these abends are accompanied by a high severity message in the SYSPRINT indicating the specific problem and possible solutions. If the SYSPRINT does not include this information, submit an error report to IBM software support.

Most abends (except some I/O related abends) are accompanied by a summary dump. When an error occurs that can be caused by a zSecure Collect problem, submit the following information to IBM software support: The error number, a copy of the summary dump shown in Figure 538 on page 1638, the JCL used, and the listing of the input commands. Figure 538 on page 1638 shows a sample

SYSPRINT log, for a CKFCOLL run that abended. The abend is indicated with a message and followed by a register dump and a traceback.

zSecure Collect prints the offset and CSECT name if the error occurs in a CKFCOLL module. The listing always includes following information: The register contents at the time of abend, a traceback with save areas, the MVS version and a processor name, the last CKFREEZE record written successfully, and the status of some internal control blocks.

```
CKRCOLL 1.9.0 06/05/07 13.19 HCKR181 I B M   T i v o l i   z S e c u r e   C o l l e c t                                page    1
 Licensed materials - property of IBM, Copyright IBM Corp. 1986-2007, All Rights Reserved

Input:  SYSIN    CRMASCH.CRMASCHD.JOB00862.D0000101.?

     1 |check=y,unix=n

CKF182I 00 Options for this run are:
           FOCUS=(RACF,AUDIT)
           IO=Y,DASD=Y,TAPE=N,SWCH=N,PATH=N,VTOC=Y,VVDS=Y,PDS=Y,CAT=Y,MCD=Y,BCD=Y,DMS=Y,ABR=Y,TMC=Y,RMM=Y,VMF=Y,UNIX=N
           RECALL=Y,SHARED=Y,OFFLINE=N,SMS=Y,STATS=N,IDR=Y,CHECK=Y,SCAN=Y
           PARALLEL=PATH,REPORT,KEY0,BYPASS,SIO,XMEM,XMDSN,DIAG,UID0,ENQ=Y,IOTIMEOUT=60

CKF047I 00 Data collection started on 19 Apr 2005 13:31 for node JES2DINO sysname DINO     sid DINO netid NLCRMM04
           on a IBM 7060 model P30
           MVSCP configuration id 09  logical partition PROD      sysplex DINORD2R
CKF039I 00 Running IBM CORP z/OS 1.4.0 DFSMS 1.3.0 JES2 z/OS 1.4
           VTAM 6.1.4/ESA  RACF 7.7.7  RMF  7.1.2    TSO 3.3.0     HSM  1.5.9
CKF130I 00 SMS system DINO configuration SMS=00 BASE SCDS
CKF111I 00 Scheduler allocated 3 I/O executors
Abend PSW 078D0000 8C28463A 00040010 6104C000 (AMODE 31)
system abend 0C4-10 (invalid storage address)
Abend at 8C28463A (at offset 04DA in routine CKFPDSE.TRCEIDR)
Data around PSW: 4110<000517FF|BFF32000>41E2
Registers at entry to abend:
R0  0C28570C R1  00000005 R2  E104C7C7 R3  0C285160
R4  00001000 R5  0C4CA7C0 R6  8C4E27A8 R7  0C4CAD98
R8  0C28A580 R9  0C4DAE58 R10 0006B850 R11 0C284160
R12 00009DC8 R13 000188E8 R14 0000001C R15 00000000
F0 0000000000000000 F2 0000000000000000 F4 0000000000000000 F6 0000000000000000
Save area at 0000A660 for procedure at 8C200000 CKRCOLL 1.9.0 06/05/07 18.50 (C) Copyright (not returned yet) R14 offset 051C
 WD1 00000000 HSA 00006F60 LSA 0000B6CC R14 8C20051C R15 0C217D80 R0  00000089
 R1  00007278 R2  0000006A R3  00007278 R4  0C2C8408 R5  0C2C8A00 R6  00AC1FE0
 R7  FD000000 R8  00AD2018 R9  00009DC8 R10 00000000 R11 8C200000 R12 00000000
Save area at 0000B6CC for procedure at 0C217D80 CKFMAIN CKRCOLL 1.9.0 06/05/07 18.30 (not returned yet) R14 offset 053C
 WD1 00000000 HSA 0000A660 LSA 0000D510 R14 8C2182BC R15 0C22B7F8 R0  002C0029
 R1  00000000 R2  0000006A R3  0006A7E0 R4  0C2C8408 R5  0C2C8A00 R6  00AC1FE0
 R7  FD000000 R8  00AD2018 R9  0000B660 R10 00000000 R11 0C217D80 R12 00000000
Save area at 0000D510 for procedure at 0C22B7F8 CKFSCHED CKRCOLL 1.9.0 06/05/07 18.38 (not returned yet) R14 offset 07F6
 WD1 00000000 HSA 0000B6CC LSA 00011758 R14 8C22BFEE R15 0C24CC08 R0  0006B9A0
 R1  F3CEE0E8 R2  0C312470 R3  0C311F18 R4  0C340790 R5  00000000 R6  0C338818
 R7  0C2F3908 R8  00AD2018 R9  0000B660 R10 0006B850 R11 0C22B7F8 R12 00000000
Save area at 00011758 for procedure at 0C24CC08 CKFPDS CKRCOLL 1.9.0 06/05/07 18.33 (not returned yet) R14 offset 007C
 WD1 00000000 HSA 0000D510 LSA 00018CC8 R14 8C24CC84 R15 0C282540 R0  0006B9A0
 R1  0C2F3908 R2  0C312470 R3  0C2F3908 R4  0C340790 R5  00000000 R6  0C338818
 R7  0C2F3908 R8  00AD2018 R9  0C24DC08 R10 0006B850 R11 0C24CC08 R12 00000000
Save area at 00018CC8 for procedure at 0C282540 CKFPDSE CKRCOLL 1.9.0 06/05/07 18.34 (not returned yet) R14 offset 03FA
 WD1 00000000 HSA 00011758 LSA 000188E8 R14 8C28293A R15 0C284160 R0  00001000
 R1  0C4CA7C0 R2  0C28A580 R3  0C2F3908 R4  0C4CA7C0 R5  0C4F7DE8 R6  0C4F86D8
 R7  00001000 R8  0C28A580 R9  0C4DAE58 R10 0006B850 R11 0C282540 R12 00000000
Save area at 000188E8 for procedure at 0C284160 CKFPDSE.TRCEIDR (not returned yet)
 WD1 00000000 HSA 00018CC8 LSA 00000000 R14 00000000 R15 00000000 R0  00000000
 R1  00000000 R2  00000000 R3  00000000 R4  00000000 R5  00000000 R6  00000000
 R7  00000000 R8  00000000 R9  00000000 R10 00000000 R11 00000000 R12 00000000
SYSPRINT buffer at time of abend (RDW=00F70000):
           VTAM 6.1.4/ESA  RACF 7.7.7  RMF  7.1.2    TSO 3.3.0     HSM  1.5.9  D2R T=60,ABR=Y,TMC=Y,RMM=Y,VMF=Y,UNIX=N

DDname   Status        Record# Source
VSM3006  Open   In         191 SM3006 CRMBHJ1.C2RNEW.SC2RLOAD(C2RACF)
IIPARMS  Closed In           1 Storage buffer length 76
CKFREEZE Open   Out      68881 SM3013 C#MASCH.C2F160T.CKFREEZE
LICENSE  Closed In          14 SM3014 C#MA.I.CNTL(CRM#CNRA)
CCPARMS  Closed Out          1 STORAGE AREA FOR TEMPORARY FILE
SYSIN    Open   In           1 C#MASCH.C#MASCHD.JOB00862.D0000101.?
SYSTERM  Open   Out          1 C#MASCH.C#MASCHD.JOB00862.D0000127.?
SYSPRINT Open   Out         80 C#MASCH.C#MASCHD.JOB00862.D0000128.?
CKF031I 00 CKRCOLL runs on DINO with MVS/SP7.0.4 DFP 3.3.2 CPU model 7060
CKF031I 00 Last record written: ID=55, contents start C3F2D7E2 D4C6E4F8 00001000

PGRP 0C340790 pathgroup 0507FFFFFFFFFFF online min=2 max=2
PGRP 0C345B08 pathgroup FDFFFFFFFFFFFFF online min=1 max=1

IOXC 0006B0A0 0344 CNSL01 pathgroup FDFFFFFFFFFFFFF state=PDS
PDS  0C2F7158 0344 CNSL01 ZSECUR.C2R110.PR21702.SC2RLOAD              trk 0082
MEMB 0C312660             CNAUDIT2 TTR 008101
IOXC 0006B850 20A4 SM3006 pathgroup 0507FFFFFFFFFFF state=PDS      <- current
PDS  0C2F3908 20A4 SM3006 C#MBHR1.C2RNEW.SC2RLOAD                     trk 0001
MEMB 0C28A580             C2RACF   TTR 000000
IOXC 000061B8 2315 ETPNT1 pathgroup 0507FFFFFFFFFFF state=PDS
PDS  0C2F36E8 2315 ETPNT1 E0515.SYS1.LINKLIB                          trk 07B2
MEMB 0C3171D0             ARCCTL   TTR 076006
CKF034I 00 CKRCOLL used 19.1 CPU seconds, 32 elapsed seconds, and collected 10.481 MB (0.324 MB/s)
           Region requested 65,536KB, granted 11,176+65,536KB
           max used in jobstep 412+3,044KB
```

Figure 538. SYSPRINT output for CKFCOLL run stopped by abend

Other Problems

The following section describes the CMD rejects problem.

CMD rejects

Sometimes, zSecure Collect causes a number of CMD rejects (unit checks) on a DASD controller (usually one per device on a specific controller). The cause is usually one of the following:

1. The z/OS system is running in a guest machine under z/VM, and the virtual machine does not have the OPTION RMCHINFO in its CP directory entry.
2. The controller tries to emulate an IBM device, but it is not compatible. That is, the controller cannot implement one of the CCWs supported by the actual IBM device. Usually this problem only occurs on OEM devices, sometimes only at specific EC levels. Submit an error report to IBM software support with a specification of the exact controller type, the job log, and the `CKFREEZE` file.

Chapter 17. Setup and Library Commands

Alert	Insight Enabler	Visual	Admin	Audit for RACF	Audit for ACF2	Audit for TSS
•	•	•	•	•	•	•

This chapter describes how to configure the menu settings and run your own zSecure queries. For information, see the following topics:

- "Start Panel - Setting your favorite menu as the entry panel"
- "SE SETUP - Options and input data sets used"
- "CO Commands - Run Commands from Library" on page 1676

Start Panel - Setting your favorite menu as the entry panel

You can specify a panel to open when the product starts. Use this function to start the product at the most convenient panel for users who typically perform a single function or small set of functions.

Note: If the administrator defined a startup panel during the product installation, contact your system administrator to request a change. Typically, users do not have the authority to modify this setting.

To specify the start panel, do the following:

1. On the command line, type `STARTPAN` to open the Start Panel selection panel.

   This panel indicates the current start panel and lists the other option panels available for selection.
2. To change the current setting, type **S** in the selection field for the new start panel.
3. Press **Enter** to apply the selection.

   The next time you start the product, this panel opens in the initial view. To go to the original Main menu, select **Main menu** from the pull-down.

Some panels have a **start panel** field or a **StartPanel** action bar item for selecting the panel as the start panel. If the panel is currently selected as the start panel, the **start panel** field is checked. Remove the selection to reset the start panel to the product default, which is typically the Main menu.

SE SETUP - Options and input data sets used

Use the SETUP menu to customize the settings and options available within Security zSecure. For example, you can select the input files for the zSecure data source and specify processing options for reporting and analysis tasks.

1. To use the SETUP menu, type `SETUP` on the command line or select the SE option from the Security zSecure main menu.

   Note: If you run the SETUP command from within a Security zSecure display, many options do not take immediate effect. They become effective on the *next* Security zSecure query.
2. Press **Enter** to open the menu.

On the SETUP menu, you only see the options you have authorization to use. The **VM Files** option is not shown in a TSO environment.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                         zSecure Suite - Setup
Option ===> ____________________________________________________________

0    Run             Specify run options
1    Input files     Select and maintain sets of input data sets
2    New files       Allocate new data sets for UNLOAD and CKFREEZE
3    Preamble        CARLa commands run before every query
4    Confirm         Specify command generation options
5    View            Specify view options
6    Instdata        Customize installation data appearance
7    Output          Specify output options
8    Command files   Select and maintain command library
U    User defined    User defined input sources
C    Change Track    Maintain Change Tracking parameters
N    NLS             National language support
T    Trace           Set trace flags and CARLa listing for diagnostic purposes
W    Windows         zSecure Visual configuration
D    Default         Set system defaults
R    Reset           Reset to system defaults
I    Installation    Specify installation defined names
```

Figure 539. Setup Menu

The Setup options described here configure IBM Security zSecure for your own user ID. You can use **SE.D** (Setup default) to configure the interface for groups of users or all users of IBM Security zSecure. This process is described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

SE.0 Setup - Run Options

The interactive component of the product keeps settings for this run and subsequent interactive runs in the ISPF profile data set. These options are set and maintained with SETUP option **0**.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Run
Command ===> ____________________________________________________________

Specify run options
Enter "/" to select option(s)
_  Use permanent work data sets  (CKRCMD is always permanent)
   _  Delete permanent work data sets on exit
_  Delete CKRCMD on exit (may contain readable passwords)
/  Allocate CKRCMD data set with RECFM=FB, LRECL=80
/  Allocate previous input files at startup
_  Suppress warning messages when appropriate input files not selected
_  Display of all status messages in sequence (degrades performance)
_  Use TSO SUBMIT (not recommended)
_  Suppress call to RACF naming convention exit ICHCNX00
_  Suppress use of RACF naming convention table ICHNCV00
_  Suppress use of RACF range table ICHRRNG
_  Touch RACF connect owner as little as possible
_  Use ACF2 masking instead of EGN

Server Token   ________
Suppress messages
Message numbers (separated by commas)
____________________________________________________________
```

Figure 540. Setup - Run panel

Use permanent work data sets (CKRCMD is always permanent)
Select this option when you want to use permanent instead of temporary work data sets. For example, when you want to use file-transfer to your workstation. See *Delete permanent work data sets* and *Delete CKRCMD* field descriptions for more information. The CKRCMD data set is always a permanent data set.

Delete permanent work data sets on exit
When **Use permanent work data sets** is selected, the Security zSecure ISPF interface allocates several work data sets for the dialog:

&WORKPREF.C2R*niiii*.CKRCMD
&WORKPREF.C2R*niiii*.CKR2PASS
&WORKPREF.C2R*niiii.CKRTSPRT*
&WORKPREF.C2R*niiii.C2RIMENU*
&WORKPREF.C2R*niiii.REPORT*
&WORKPREF.C2R*niiii.SYSTERM*
&WORKPREF.C2R*niiii.SYSPRINT*

For efficiency reasons, the WORKPREF data sets are not deleted when you are finished with the dialog. Use the **Use permanent work data sets** option when security or space management considerations require that you delete these data sets after leaving the interface. The CKRCMD data sets are only deleted if you select the suboption **Delete CKRCMD on exit** as well.

Note: For additional information about the WORKPREF configuration parameter, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Delete CKRCMD on exit (may contain readable passwords)
Because the CKRCMD might contain sensitive information, only select this

option when Erase-on-scratch is active. Otherwise, a disk scavenger program can find the readable passwords in the tracks of the deleted data.

Allocate CKRCMD data set with RECFM=FB, LRECL=80
Select this option to allocate the CKRCMD data set with RECFM=FB,LRECL=80 instead of RECFM=VB,LRECL=255. For new users, RECFM=FB, LRECL=80 is preselected as the default.

Allocate previous input files at startup
If you select this option, the dialog startup automatically allocates the input data sets you last selected with option SETUP FILES. Otherwise, the installation default allocation is used (if any).

Suppress warning messages when appropriate input files not selected
When an option needs a specific input source such as a CKFREEZE file that is not allocated by the selected set of input files (option SETUP FILES), a message is issued. When a batch run is requested, you can choose to continue the query and allocate the required source via the IBM Security zSecure submit menu (Select an alternate set of input files). If an online query is requested, the option or selection is not selectable. This option can be used to suppress this behavior.

Display of all status messages in sequence (degrades performance)
This option causes all available ISPF status messages to be displayed even though this degrades performance. Normally (off), a status message is only displayed if sufficient time has elapsed since the previous one. This option can be helpful for automated testing or for debugging purposes.

Use TSO SUBMIT (not recommended)
Select this option to call TSO SUBMIT instead of the `C2RSUB` program. Using TSO SUBMIT can result in truncation or continuation problems because that program does not support long records. However, you might want to use TSO SUBMIT because `C2RSUB` does not provide a job card and does not call the site SUBMIT exit.

Suppress call to RACF naming convention exit ICHCNX00
By default, zSecure Admin and Audit calls the system RACF naming convention exit. Selecting this option suppresses these calls. This option can be useful when processing data from another system because the ICHCNX00 of the current system is used, not that of the subject system. This suppression option is not allowed in restricted mode.

Suppress use of RACF naming convention table ICHNCV00
By default, zSecure Admin and Audit simulates processing of the system RACF naming convention exit. Selecting this option suppresses this behavior. However, this suppression is not allowed in restricted mode. Suppressing this option might be useful when processing a database copy or an unload file from another system without a proper `CKFREEZE` file.

Suppress use of RACF range table ICHRRNG
Selecting this option disables use of the system RACF range table. This option is useful if you do not have the proper CKFREEZE file for a RACF database copy, and hence no proper ICHRRNG. You can also consider using this option when you want to find errors in the way a database is split across multiple data sets, errors such as profiles that are defined in the wrong data set, and hence are not used by RACF. Use of this option can lead to *duplicate profile*, *class not in CDT*, and *connect inconsistency*' messages.

Touch RACF connect owner as little as possible
The connect owner field is formally obsolete. If it is not in use for site-specific purposes, consider suppressing its maintenance to improve program

performance. When this option is selected, the program ignores the connect owner field of user profiles during VERIFY PERMIT, REMOVE PERMIT, and MERGE operation. For VERIFY PERMIT and REMOVE PERMIT, setting this option means that zSecure does not generate CONNECT commands to change the connect owner when it is a userid or group which no longer exists.

For MERGE operations, commands are not generated to make the connect owner in the CURRENT database the same as the connect owner in the MERGESOURCE database.

Use ACF2 masking instead of EGN
Use this option to set MASKTYPE to *ACF2*. MASKTYPE sets the way filters are interpreted. The mask type can be *EGN* or *ACF2*. The default is *EGN*. This option is available only when both Admin or Audit for RACF and Audit for ACF2 is installed.

Server Token
Specifies the suffix for the name of the name/token pair that is used to locate the program call (PC) information for a zSecure server. The default value for the server token is PRODSERV. If you specify a value for this keyword, it must be 8 characters or less. Specifying a value for this keyword is required only if you are running multiple zSecure servers on the same system, or if the value for the zSecure server has been changed from its default value.

Suppress messages
You can use this field to suppress messages when they are no longer required to be included in reports. Enter a comma-delimited list of numbers for the messages to be suppressed. You only need to specify the message number, not the full message ID (CKR*nnnn*). Leading zeros are not required.

Suppressed messages do not contribute to the maximum return code.

SE.1 Setup - Input files

As mentioned in “Data Sources” on page 2, IBM Security zSecure processes data from the following sources:

- Data from your security system

  This data set can be the active RACF database, unloaded RACF data, a copy of a RACF database, or an active RACF database from another system.
- Data describing your system configuration (control blocks and DASD)

  This data resides in a CKFREEZE file.
- Data describing events on your system (SMF and other sources)

These data sources must be grouped into **sets** to provide input data for the interactive component of Security zSecure. A **set** is the unit that you can select or unselect for use. Each set can contain one or more data sets. You can create, edit, and delete sets using the Setup Files function. When creating or editing a set, assign the set to a **complex** which represents a group of system images (z/OS or z/VM) that share a security database. Typically, a complex contains that security database and the CKFREEZE files for all or some of the system images that share it. A complex can also contain event data, such as SMF data used for reporting on the events recorded on the systems included in the complex. Event data is only used by the Audit component of IBM Security zSecure. A complex must include at least one input data set which can be a security database, a CKFREEZE file, or SMF event data, but it can contain multiple input data sets.

Note: Information about creating and refreshing an UNLOAD and CKFREEZE data set, see "Refreshing an UNLOAD or CKFREEZE data set" on page 1652 and "SE.2 Setup - New files" on page 1653.

The complex name is used whenever the COMPLEX field is included in queries, on the USER display for example. If the Complex name is not specified, the default value is used. The default value depends on the specified input data source. For data from an UNLOAD operation, the value is the name of the unloaded database. For live data, the default is the name of the live system that is supplying the data. If no unload or live security database is present, a CKFREEZE file is used. In restricted mode (see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*), a complex name cannot be different from the actual system name that would be used as the default. When not in restricted mode, the complex name can be used as you see fit.

There are three different types of input sets within Security zSecure. Each set has specific rules for changing the field values.

SYSTEM-DEFINED SETS
If no input sets are defined, Security zSecure defines three default input sets for the *active primary*, the *active backup*, and the *active backup + active SMF* input set. You can only delete the default set definitions if other sets have already been defined. The Delete function is available from the **SETUP DEFAULT** option. The default system definitions are restored to the list of available inputs when a **reset to system defaults** action is performed, either implicitly or explicitly.

DEFAULT SETS
You can define default sets for all new users as described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. These default sets can only be changed through the SETUP DEFAULT option, not by the individual user. If default sets are defined, the default definitions are restored to the input data sets when a reset to system defaults is performed, either implicitly or explicitly.

USER SETS
Users can define their own input data sets from the Setup - Input files panel. The user can change the definition for these user-defined data sets at any time. The user-defined input sets are **not** affected when a **reset to system defaults** is performed.

To use the Setup Input option to specify the data sources for zSecure, do the following:

1. Type SE.1 on the command line or select the **Input files** option from the main menu.
2. Press **Enter** to open the Setup Input Files menu shown in Figure 541 on page 1647 .

```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                        zSecure Suite -Setup - Input files
Command ===> _____________________________________________ Scroll ===> CSR

(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

  Description                                                  Complex
_ Active primary RACF data base                                C##4     selected
_ Active backup RACF data base                                 C##4
_ Active backup RACF data base and live SMF data sets          C##4
_ User defined set                                             testcomp
****************************** BOTTOM OF DATA *********************************
```

Figure 541. Overview of input files sets

The default RACF database shown on the Setup - Input panel is the one that your installer or system administrator specified in the zSecure configuration file. This database might or might not be the active database.

Table 647 provides a list of the line commands available to manage the Input file sets.

Table 647. Setup Input files panel - available line commands

Task	Command	Description
Select an input set for processing	**S**	When you select an input set, the data sets it contains are selected for processing. After the data sets have been located in the system, the set is marked as **selected**. This option is also selected by specifying A. The selected set is an addition to sets already selected.
Remove an input set from selection	**U**	When you remove the selection from an input file set, the data sets are not used in future queries.
Browse a set of input files	**B**	Check the definitions for the set. When you exit the detail panels, the set is not selected.
Edit the data sets included in an input set.	**E**	When you enter this command, the list of data sets included in the input set are displayed so you can change them. If you press **F3** or enter `END` on the Edit panel, the set is marked as **selected**.
Copy the contents of an existing input set to a new input set.	**R**	Repeat a set. The contents of the set you choose are copied into a new set. The new set is shown. If you press **F3** on the panel showing the new set, it is selected for processing as if you had entered the **S** line command.
Insert a new input set.	**I**	Opens a new input file set where you can add the desired data sets to be included as input sources. After you enter the data set information and press F3, the new input set is selected for processing.
Delete a data set.	**D**	Removes an input set entry or a data set entry in the input set definition. The name and associated information are removed from the view. However, the data sets in the set are not deleted from the system. The D line command is not available for system defined and default sets.
Refresh the data sets included in the input set.	**F**	Entering this command opens a panel that allows you to submit a job to refresh the contents of the data sets. The **F** line command is not available for system-defined and default sets.

You can select multiple input sets for processing. The input sets can be associated with the same complex or with different complexes. However, for any complex in the combined sets, you cannot have more than one security database, be it active primary, backup, or unload.

To exit the Setup Files function, you can either press the **END** key, the **PF3** function, or enter the **CANCEL** command. Using the end key, saves the current settings in your ISPF profile. When you exit, a message is displayed indicating which complexes are selected. The selected input complexes are also displayed at the bottom of the main menu.

When you edit or create an input file set, the panel shown in Figure 542 opens:

```
   Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                        zSecure Admin and Audit - Setup - Input files
Command ===> ____________________________________________________ Scroll ===> CSR_

Description . . . . Your description for this set of input files
Complex . . . . . . ________   Version  . . . .  ____
RRSF node . . . . . ________   Local node for RRSF

Enter data set names and types.         Type END or press F3 when complete.
Enter dsname with .* to get a list      Type SAVE to save set, CANCEL to quit.
Valid line commands: E I R D            Type REFRESH to submit unload job.

Data set or DSNPREF= or UNIX file name                    Type        NJE node
_ ____________________________________________________ ___________ ________
****************************** Bottom of data ********************************
```

Figure 542. Initial view of an input file set under z/OS

On this panel, you can add data sets or files for the specified input set. You can enter data set names with or without quotes. The TSO PREFIX is put in front of an unquoted data set name. Trailing quotes are automatically supplied. Generation data sets in relative notation and full GDGs are supported. For a full GDG, you can specify the GDG base name without any member selection. This specification concatenates all data sets belonging to the GDG. Full GDGs cannot be used for security databases or CKFREEZE data sets.

When using relative GDG data sets or full GDGs, make sure that you understand the serialization effects. For example, MVS guarantees that `YOUR.GDG(-1)` refers to the same data set throughout your job or session. Consequently, after you have allocated a relative or full GDG to your zSecure session, a job that tries to create a generation can fail or wait until your session has finished.

To allocate all data sets with a specified High-level qualifier, specify the value for the qualifier in the **DSNPREF** field. For example, if you specify `DSNPREF=SYS1.DAILY.SMF` all data sets that are allocated begin with the High-level qualifier `SYS1.DAILY.SMF`. The last qualifier specified is interpreted as a partial qualifier. If you want to match only full qualifiers you have to end the `DSNPREF` value with a period. The `DSNPREF` parameter value is resolved immediately before reading the data which can result in having different data sets allocated each time. As a result, the Setup Input transaction does not test for missing or migrated `DSNPREF` data sets.

If you specify the `DSNPREF` parameter, you cannot specify values for the `UNIT` and `VOLUME` fields.

Instead of OS data set names, you can use UNIX path names. When you want to allocate SMF log streams you enter the log stream name here, optionally followed by a SUBSYS parameter. For example, to get all records from Oct 15, 2007, you can use the following specification:

```
IFASMF.MAIN('FROM=(2007/288),TO=(2007/288),LOCAL')
```

The input field only allows 55 characters. If you need more, you must code the CARLa ALLOC statement yourself. For additional information, see "ALLOCATE" on page 718 and the *z/OS MVS JCL Reference*.

On this panel, enter file names according to ISPF standards. To search for files, specify a file name ending in `.*`. Then press **Enter** to display the matching filenames. On the resulting display, you can remove the entry for the generic specification (`.*`) and any other files that you do not need by entering the `D` line command. The delete command does not delete the data set, it just removes the name and information from the display.

This **Version** field can be used to classify the data allocated into separate sets like OLD and NEW. This value is different than the COMPLEX value, which is used to identify the systems with a shared security database that are the source of the data. You can use the VERSION specification to analyze data in the same COMPLEX at multiple points in time.

Many reports only show 8 characters of the complex name, which does not include the VERSION identifier. If you use the same COMPLEX name, you cannot use the report to identify the data from different versions.

To insert a new data set, use the **I** line command.

On the panel in Figure 541 on page 1647, you can also specify the **Type** for the input data source. Table 648 lists the available data set types.

Table 648. Input Files: available data set types

If you want to use...	use TYPE...	Notes
The primary RACF database of your active system	`ACT.PRIM`	2 8
OS RACF database	`COPY.RACF`	8
The live SMF data sets	`ACT.SMF`	2
The backup RACF database of your active system	`ACT.BACK`	1 8
An unloaded security database	`UNLOAD`	
A copy of a single-dataset RACF database (for example, restored, or from a different system image)	`COPY.RACF`	8
A copy of a multi-dataset RACF database (for example, restored, or from a different system image)	`COPY.TEMP`, `COPY.SEC`	3
Live settings	`ACT.SYSTEM`	4
A CKFREEZE data set	`CKFREEZE`	
VSAM or dumped SMF	`SMF`	5
SMF log stream	`SMF.LOGSTR`	5
An ACCESS monitor data set	`ACCESS`	Admin only

Table 648. Input Files: available data set types (continued)

If you want to use...	use TYPE...	Notes
The access log of a webserver	WEBACCESS	Audit only
The error log of a webserver	WEBERROR	Audit only
Other event logs	<deftype>	6
A file for generated RACF commands	CKRCMD	7

Notes:

1. The data set name for the RACF database is not required.
2. Audit only. The data set name is not required.
3. Sequence is important for a multi-dataset RACF database. In ICHRDSNT, the first data set of the systems where this is or was the active database must have type COPY.TEMP because that data set contains the RACF templates that are used on that system. The other data sets have type COPY.SEC, and must be specified in the same order as in ICHRDSNT.
4. If you process multiple complexes and *complex A* does not contain a CKFREEZE data set while *complex B* and *C* do, *complex A* inherits one of the available CKFREEZE data sets from *complex B* or *C*. This inheritance causes unpredictable results. The ACT.SYSTEM type authorizes you to explicitly tell the program to use the current live settings for this complex instead of the settings from a CKFREEZE data set.
5. Audit only. Intermediate data sets from RACFRW or the IRRADU00 SMF unload program are not supported.
6. You can use the **SE.U** option to create your own types of data sources. For details, see "SE.U SETUP - user-defined input sources" on page 1667. You can use the DEFTYPE name assigned to your data source using the SE.U function as the **Type** on the **SE.1** menu.
7. Admin only. This file is used for output. If you do not supply a CKRCMD file, a work file is created as needed. If you create it yourself, it must be a sequential data set with record format FB and record length of 80 bytes, or a sequential data set with record format VB and record length of 255 bytes. Any previous content is overwritten. After commands have been generated here, you have options to run the commands, save them, submit a job, and so on.
8. Using a RACF database that is in active use (either as database of the life-of-job system, or as a foreign database) incurs the risk that the database is updated by RACF while zSecure is reading the database. To avoid this risk, use an UNLOAD data set.

When not certain of the Type, you can enter a question mark in the **Type** column. Then, press **Enter** to display a list of supported types as shown in Figure 543 on page 1651.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
Security zSecure Admin and Audit for RACF - Setup - Input files   Row 1 to 13 of 13
Command ===>_____________________________________________________ Scroll ===> CSR_

 Select the type of data set or file
     Type            Description
_    ACCESS          RACF ACCESS monitor data set
_    ACT.BACK        The backup RACF database of your active system
_    ACT.PRIM        The primary RACF database of your active system
_    ACT.SMF         The live SMF dataset(s)
_    ACT.SYSTEM      Live settings
_    CKFREEZE        System resource information data set
_    CKRCMD          A file for generated RACF commands
_    COPY.RACF       A copy of a single-dataset RACF database
_    COPY.SEC        A non-first component of a multi-dataset RACF database
_    COPY.TEMP       The first component of a multi-dataset RACF database
_    SMF             VSAM or dumped SMF
_    SMF.LOGSTR      SMF logstream
_    UNLOAD          An unloaded RACF database
_    WEBACCESS       IBM HTTP Server access log
_    WEBERROR        IBM HTTP Server error log
****************************** Bottom of data ********************************
```

Figure 543. File type menu for Setup files

On the panel shown in Figure 541 on page 1647, you can select the type that applies to your input. Press Enter to return to the previous screen.

You can also specify an NJE node to refresh the UNLOAD data set and/or CKFREEZE data set. Refresh needs to run on a system that the to-be-refreshed data pertains to. For an UNLOAD data set, this value can be any of the systems that share the security database. For a CKFREEZE data set, the refresh must run on the system that is described by the CKFREEZE data set. If the target NJE node is a Multi-Access Spool node, you also need to specify the system within that node. To specify the system for the node by use the **E** line command on a data set

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
           Security zSecure - Setup - Input files
 Command ===> _____________________________________________ Scroll ===> CSR_

 Description . . . . Set_of_files_for_development_system_____________________
 Complex . . . . . C##4____   Version  . . . .  ____
 RRSF node . . . . . ________  Local node for RRSF
 Enter data set names and types.         Type END or press F3 when complete.
 Enter dsname with .* to get a list      Type SAVE to save set, CANCEL to quit.
 Valid line commands: E I R D            Type REFRESH to submit unload  job.

 Data set or UNIX file name                                Type        NJE node
 e 'PRODBRP.ZSECUR.UNLOAD'_________________________________ UNLOAD_____ ________
 _ 'PRODBRP.ZSECUR.CKFREEZE'_______________________________ CKFREEZE___ ________
****************************** Bottom of data ********************************
```

Figure 544. Zooming in to a data set within a set of input files

After you press **Enter**, the panel shown in Figure 545 on page 1652 opens so you can specify both the NJE node and system within that node.

```
Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        Security zSecure - Setup - Input files
Command ===> ____________________________________________________________

Description . . . . Set of files for development system
Complex . . . . . C##4____ Version  . . . .  ____
RRSF node . . . . . ________   Local node for RRSF
Dataset name  . . . 'PRODBRP.ZSECUR.UNLOAD'
Volume  . . . . . . ______
Unit  . . . . . . . ________
Type  . . . . . . . UNLOADNJE node  . . . . . ________   /*XEQ parameter
System name . . . . ________   /*SYSTEM parameter
zSecure Node name . ________   Name of remote zSecure Node
zSecure System  . . ________   Name of remote zSecure System
Function  . . . . .   1. Main     2. Base
****************************** Bottom of data ********************************
```

Figure 545. Specifying data sets details within a set of input files

This same panel can also be used to access non-cataloged data sets. This function is not supported for VSAM or SMS-managed data sets.

On the panel in Figure 541 on page 1647, you can also specify an RRSF (RACF Remote Sharing Facility) node. This field indicates the node used in command generation. It is directly related to the Complex field. The RRSF node can be defined using the Edit line command on the Setup - Input Files panel.

You can also specify the name of remote **zSecure Node** and the name of the remote **zSecure System**. See *Multi-System Support* for more information.

In addition, you can specify a value for the **Function** field:

1. Main
For UNLOAD files, this value indicates that the database is to participate normally in VERIFY and REPORT commands. This setting is the default used if the Function field value is not specified.

2. Base
Select this option to automatically activate compare mode for detecting and reporting on changes in selected fields. All identical records from different complexes are suppressed. This specification works best when multiple data sets for different complexes are used. Only one data set of the same TYPE can specify function=base. See "Compare processing" on page 46.

Note: If two or more ALLOC statements specify the same COMPLEX but one has FUNCTION=BASE the other cannot have FUNCTION=MAIN.

Refreshing an UNLOAD or CKFREEZE data set

On the Setup - Input Files panel (Figure 541 on page 1647), enter the **F** line command to refresh an UNLOAD or CKFREEZE data set. When you enter the command, zSecure generates a batch job and opens a panel to submit the job. You can browse or edit the batch job, or include the generated job in your production schedule.

When the job runs under a system other than your local system, it is assumed that an NJE connection is in place. If an NJE connection does not exist, capture the job and transfer it using another method. It is also assumed that you have shared DASD which means that the data refreshed on the target system is immediately available on your local system. If you do not have shared DASD, use another method to transfer the refreshed data back to your local system.

SE.2 Setup - New files

This function can be used to create and fill new UNLOAD and CKFREEZE files. You can set up these data sets on the panel shown in Figure 546.

```
 Menu   Options   Info   Commands
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - New files
Command ===> ____________________________________________________________________

Create new unload file from the RACF database and CKFREEZE file


Dataset with unload from RACF database, use UNLOAD as last qualifier
 Unload . . . . . myname.unload_____________________________

I/O configuration file, use CKFREEZE as last qualifier
 Ckfreeze . . . . . myname.ckfreeze_____________________________

Description for this set of input files
 Description  . . . private set of unloaded files_____________________


Enter data set names and description and press ENTER
******************************* Bottom of data ********************************
```

Figure 546. Setup - New files panel

Data set names must conform to TSO conventions. Use quoted data set names if needed. Use *UNLOAD* or *CKFREEZE* as the last qualifier in the data set name, as shown in 1653. If you use these qualifiers, the **SETUP FILES** (**SE.1**) function automatically recognizes the types. When you press Enter, the program checks to determine whether each data set is cataloged. If a data set cannot be found, the allocation entry panel is displayed.

```
 Menu   Options   Info   Commands
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - New files
Command ===> ____________________________________________________________________

CKFREEZE file not found. Change dataset name, or specify allocation parameters

 Dataset name . . . MYNAME.CKFREEZE_____________________________

Allocation parameters to create new dataset:
 Volume serial  . . ______      (Blank for authorized default volume)
 Generic unit   . . ________    (Generic group name)
 Space units  . . . _____       (KB, TRKS, or CYLS)
 Primary quantity   ________    (In above units, press HELP for suggestion)
 Secondary quantity ________    (In above units)

 Record format  . . VBS__       (VB or VBS)
 Block size   . . . 27998__
 Logical Record Len X______     (X or maximum record length)

Press ENTER to allocate dataset, press END to stop processing
```

Figure 547. Setup - New Files Allocation Entry panel

Specify sufficiently large space parameters for new data sets. Recommended values are:

CKFREEZE
2 megabyte per on-line DASD volume

UNLOAD
Specify a value equal to the size of your RACF database

After the data sets have been created, they are put into a set, and Figure 544 on page 1651 will be shown, inviting you to enter the REFRESH command on the command line. This procedure is described under "SE.1 Setup - Input files" on page 1645. You can start using the new set once the REFRESH job is successfully completed.

SE.3 Setup - Preamble

Use the PREAMBLE function for setting up common commands used in every action or query. For example, if your installation considers **all** link list data sets sensitive instead of just the APF data sets, you can add a SIMULATE SENSITIVE LINKLIST statement to every run. The PREAMBLE provides a simple way to customize the product. You can add an INCLUDE command in the preamble to add a user or installation-defined member to every run.

You specify the preamble commands from the Setup - Preamble panel shown in Figure 548.

```
 Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                        zSecure Suite  - Setup - Preamble
Command ===> ____________________________________________________________

_  Execute preamble commands before every query

Enter CARLa commands below (no conversion to UPPER case):
>
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
> ____________________________________________________________________________
```

Figure 548. Setup - Preamble

To use the preamble commands each time a query is run, select the **Execute preamble commands before every query**.

Execute preamble commands before every query Use this option for including the Commands entered on the Preamble panel in every call to the program. You can temporarily disable the Preamble function by removing the selection (/) from the **Execute preamble commands before every query** on the panel. If no commands have been specified, this field is not selected.

For more information, see "Using the Preamble function."

Using the Preamble function

This example shows how to suppress a user or group ID on the profile displays. In this case, the user or group ID is one that is included on the access list for all DATASET or general resource profiles in your installation.

You can use the following PREAMBLE statement to accomplish this task:

```
DEFINE ACL SUBSELECT,
       ACL(ID<>(IBMUSER,SYSAUDIT) OR ACCESS<>ALTER)
```

The statement can be defined in a PREAMBLE statement, either individually on the Setup - Preamble panel, or using the Setup Default function available on the Setup menu.

This statement redefines the ACL output variable to show only access list entries that do not specify the *IBMUSER* or *SYSAUDIT* IDs with an access level of ALTER. If one of these IDs has another access level it is shown. This modified ACL output variable is used in all displays where the variable is not redefined again.

Notes:

1. The ACL redefine does not influence the REPORT command. Reports produced from option **3** still contain the suppressed IDs.
2. Commands generated to clone data set profiles by typing a *C* in front of a profile use the ADDSD XXX FROM(YYY) construction. In this case, the new profile contains the same access list as the original profile, plus the user ID used to run the command.
3. Only the **ACL**, **CONNECTS** and **USR** fields can be redefined in this way. For more information, see "DEFINE" on page 750.

SE.4 Setup - Confirm

Use the Setup Confirm option to specify command execution options. These options specify:

- How commands are executed, for example, immediately or queued.
- How you are prompted for command routing information.
- If generated commands must be confirmed before execution.
- If certain field values can be modified, if authorized.
- Which types of commands can be generated.

Note that some options can also be set from within a display panel using the SET command.

```
 Menu         Options       Info    Commands     Setup
_____________________________________________________________________________
                          zSecure Suite - Setup - Confirm
Command ===> _____________________________________________________________

Action on command . . 2  1. Queue    2. Execute  3. Not allowed
                         Execute display commands (for option 1 only)
Confirmation  . . . . 4  1. None     2. Deletes  3. Passwords      4. All
Command Routing . . . 3  1. Ask      2. Normal   3. Local only

Command generation
Enter "/" to select option(s)
/  Overtype fields in panels
/  Change generated commands
/  Specify start/end date
/  Generate SETROPTS REFRESH commands
   / Issue prompt before generating SETROPTS REFRESH commands
Commands to generate
/  RACF commands
/  CKGRACF commands
/  CKGRACF ASK for later execution
/  CKGRACF REQUEST for later execution
_  CKGRACF WITHDRAW queued commands
/  CKGRACF RDELETE commands
```

Figure 549. Setup - Confirm

Action on command

Use this field to specify what actions to take for the line commands and overtypes. For example, you can specify whether to write the commands generated by line commands and overtypes to an output file or run them immediately. Table 649 lists the available options.

Table 649. Setup - Confirm panel - Action on command options

Action setting	Description
Queue	TSO commands are written to an output file (CKRCMD) for later use.
Execute	TSO commands are run immediately after confirmation.
Not allowed	For zSecure Admin, users cannot issue line commands and fields cannot be modified from the interface. For zSecure Audit, line commands cannot be used.
Execute display commands (for Queue setting only)	For display or list commands only, such as LISTUSER, PING, TRACERTE, and RLIST, select this option to execute list commands for the Queue action setting. The option to override the queue setting and execute list commands applies to generated list commands only and does not change the execution of any list commands that you enter. For example, a list command entered with the FORALL command is not effected by this option.

If a single command is generated, for example, when you change a value on a display panel, or use certain line commands, zSecure can be set to display a confirmation panel showing the generated command. If multiple commands are generated, for example, when you use the Copy or Recreate line command, zSecure does not display a confirmation panel. In this case, if confirmation is set to All or Delete and Action is set the Execute, zSecure queues the commands so that they can still be confirmed.

If Action is set to queue, or zSecure queues multiple output commands because Action is set to Execute, the generated commands are written to the CKRCMD

command file. See “A sample run” on page 17 for an example. When you exit the display panel, the CKRCMD file is displayed in an EDIT session. You can then inspect the generated commands and change them to meet your site requirements.

When you exit the edit session, the Results panel is shown. See “A sample run” on page 17 for an example. This panel provides the following options:

- Run the commands.
- Write them to a file.
- Submit the commands, possibly to a different system image.
- Discard the commands.

Notes:

1. Commands generated from the **Quick User Administration (RA.Q)** option are always executed directly.
2. In zSecure Admin, creating a profile or segment also bypasses confirmation. The confirmation settings apply only to the dialog that updates the profile or segment that was created.
3. If the commands contain line commands on profiles, the commands are queued for CKR2PASS and are not always automatically shown on the Results panel. You can view or edit these commands from the Results panel, unless you have set the Confirmation option to None. In this case, the CKR2PASS output is immediately run as a second-pass CARLa. (For information about CKR2PASS commands, see “RESULTS - View output and results” on page 24.)

Confirmation

In zSecure Admin, this option determines if commands that are generated must be confirmed before they are queued or run. Table 650 describes the available options.

Table 650. Setup - Confirm panel - Confirmation command options

Confirmation setting	Description
All	Commands must be confirmed.
Delete	Only commands that perform a delete action must be confirmed.
Password	Commands with a readable password or password phrase must **not** be confirmed.
None	Commands are never confirmed.

Command Routing

The three routing levels are:

Ask

This option sets the maximum prompting level. For all commands or command files, the user is prompted for command routing information. This setting applies to commands generated for the local system, as well as for commands generated from data sources that are known to be from other systems.

If Command Routing is set to **Ask**, you are asked to select command destinations before the command is executed. For more information, see “Command routing” on page 28.

Normal
This is the default prompting level. Commands are run without prompting for command routing options. Confirmation prompting and command queuing is done according to the user settings. If you want to queue commands instead of executing them, choose the Queue option on the Confirmation panel that displays at during program operation. If the RACF data source applies to the local system, commands are routed to the local system. The user can specify remote options for the following local data sources: RRSFNODE, ZSECNODE , or JESNODE). These remote indicators are ignored for a local data source. If the commands are not for the local system, they are routed to one of the following systems in order of preference:

1. The zSecnode or the zSecsys as specified by the RACF data source used for this profile.
2. The node specified in the RRSFNODE for the RACF data source used for this profile. The command uses the AT keyword, specifying either the current userid or the associated userid if the terminal user has an association with a userid on the target RRSFNODE.
3. The JES node specified for the RACF data source. If a specific routing mechanism is selected and fails, there is no automatic fallback to another routing mechanism.

Local only
This is the old method of command routing. The command is routed to the local system independent of the input source. If the local system is part of an RRSF autocommand environment, RRSF processing might route this command to other RRSF nodes.

Command Generation
The following options determine how commands are generated and processed.

Overtype fields in panels
Check this option to provide the option to type over values in fields on a display panel. Changing field values generates RACF commands to complete the change in the RACF database.

Change generated commands
This option specifies whether you are allowed to change commands after they have been generated. If a change is required to complete the command, this option is ignored. For example, if you run a Copy command on a profile, a change is required. The user must specify a name for the profile copy before saving it.

Specify start/end date
If this option is checked, you are prompted for a start and end date when generating CKGRACF commands.

Generation SETROPTS REFRESH commands
If selected ("/"), this option specifies that SETROPTS REFRESH commands can be generated. If it is not selected, the refresh command generation is suppressed.

Note: If SUPPRESS SETROPTS REFRESH is specified in the Preamble, this option is ignored. For more information, see "SE.3 Setup - Preamble" on page 1654 and "SUPPRESS" on page 932.

Issue prompt before generating SETROPTS REFRESH commands
If this option is selected ("/"), the *Action on command EXECUTE* is in effect. As a result, and SETROPTS REFRESH commands are generated. You are

prompted to decide whether to issue the commands. If this option is not selected, the prompt for the SETROPTS REFRESH command generation is suppressed.

Commands to generate
The following options determine which commands can be generated.

RACF commands
This option specifies that RACF commands can be generated when a command is run. If there are other command types, you are prompted to specify your preference for command generation.

CKGRACF commands
This option specifies that CKGRACF EXECUTE commands are generated if required. The only advantage of using this option instead of the *RACF commands* option is that you can specify a REASON that is written to SMF together with the command in an extra audit record.

CKGRACF ASK for later execution
Use this option for generating the `CKGRACF ASK`[24] command so it can be submitted for processing at a later time.

CKGRACF REQUEST for later execution.
This option specifies that a CKGRACF REQUEST command can be generated.

CKGRACF WITHDRAW queued commands [24]
This option specifies that a CKGRACF WITHDRAW command can be generated.

CKGRACF RDELETE commands
This option specifies that a CKGRACF RDELETE command can be generated when a delete action is requested for a DATASET or general resource profile.

SE.5 Setup - View

Use the view menu to specify the amount and appearance of the data presented to you. The access list settings can also be set from a display panel using the `SET` command.

24. For details on the exact meaning of and differences between CKGRACF EXECUTE, ASK, REQUEST, and WITHDRAW commands, see "CMD" on page 1505.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                     zSecure Suite - Setup - View
Command ===> ____________________________________________________________

 Access list format . . . . 2  1. No       3. Explode  5. Effective
                               2. Sort     4. Resolve

 ACL/Connect sort . . . . . 2  1. Id       2. User     3. Access
 Show OS specific options   /  z/OS        _  z/VM
 /  Add user/group info to view
     (Selecting this will use some additional storage - normally on )
 /  Add summary to RA displays for multiple complexes (normally on)
 _ Add connect date and owner to RA.U connect group section

 Select view
 3  1. View only profiles you are allowed to change (administrator view)
    2. View all profiles you are allowed to change or list
    3. View all profiles (normal view)
```

Figure 550. Setup View Panel

Access list format

Determines the layout of access lists fields. Select 1. No to suppress the access lists. Select the SORT to sort the access list.

Table 651. Setup - View panel - ACL list field layout options

Action setting	Description
EXPLODE	Display the access list in sorted and exploded format. When this option is selected, the view includes information about all possible ways the user has access.
RESOLVE	Display the access list in sorted and resolved format. This layout only includes the most specific way that a user has access in the view.
EFFECTIVE	Also shows users that are not on the access list but have access due to operations or group operations privileges. Specifying `EFFECTIVE` switches on full database read instead of indexed access, which can result in increased query response time. Although full database read is turned on, you still might not be able to see all connects and operations users. Some information can be missing if universal group connects are not fully expanded. To guarantee that all access is shown for the RA.D or RA.R functions, use the Enable full ACL option.

Use the `SORT` value for the Access list format. This configuration enables the C line command as well as permitting you to change the values in the access list entries without significantly increasing query response time.

ACL/Connect sort

This option determines the sort order of access list and connect displays. The sort order is used with the `SORT`, `EXPLODE`, `EFFECTIVE`, and `RESOLVE` options. The following table lists the possible values for this option.

Table 652. Access List and Connect displays: Available sort orders

Value	Description
ACCESS	Sort by access level, from `ALTER` to `NONE`. For connects, `ACCESS` means sort by the following descending access settings: non-revoked, group-special, group-operations, group-auditor, and join, connect, create, and use authority.

Table 652. Access List and Connect displays: Available sort orders (continued)

Value	Description
ID	Sort by unresolved, unexploded access list `ID`. For connects, `ID` means sort on the `ID` in the connect list.
USER	Sort by exploded or resolved access list `ID`. For connects, `USER` means sort on the id in the connect list.

Show OS specific options
With this option you can switch between z/OS and z/VM specific options, or tag both to see all options.

Add user/group info to view
When this option is selected, the display panels for user profiles and group profiles includes information about users and groups on access list and connect displays. Selecting this option does increase the amount of virtual storage being used because of the added user and group information. If this option is not selected, the options for issuing **C** (Copy) line command and modifying the connect and access list information are not available. Leave this option selected unless you have severe memory constraints.

Add summary to RA displays for multiple complexes
When this option is selected, an extra summary section is added to the display panels for the following options RA.U, RA.G, RA.D, and RA.R. The summary information shows profile differences when multiple complexes are selected. This setting is not saved in your ISPF profile. This option is enabled by default.

Add connect date and owner to RA.U connect group section
Use this option to add the connect date and connect owner to the RA.U connect group section.

Select view
Use this option to specify which profiles are displayed.

- **View only profiles you are allowed to change** requests to show only profiles that you can modify.
- **View all profiles you are allowed to change or list** requests to also show profiles in your CKGLIST scope or within your group-AUDIT authority.
- **View all profiles** is the typical, most efficient view option because it saves storage and CPU time. If you are not running in restricted mode, setting this option can make a noticeable difference in response time and storage requirements.

SE.6 Setup - Instdata

Use the Setup `Instdata` option to maintain `instdata` mappings. After you have added an `instdata` definition set, you can specify different `instdata` mappings for the USER, GROUP, DATASET, and RESOURCE classes. You can use the defined fields for creating an output layout. Different layouts can be created for the overview and detail displays as well for the print formats.

1662 shows a table of `instdata` definition sets:

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                     zSecure Suite - Setup - Instdata     Row 1 to 2 of 2
Command ===> _____________________________________________ Scroll ===> CSR

Select INSTDATA definition set ( S (select), U (unselect),
E (edit), I (insert) or D (delete))


    Name       Description
_   PROD       Production LPAR                          Active set
------------------------------------------------------------------------------
_   DEV        Development LPAR                         _________
------------------------------------------------------------------------------
****************************** Bottom of data ********************************
```

Figure 551. Setup Instdata panel

You can use the following line commands on this display:

Table 653. Setup Instdata panel - available line commands

Command	Description
S	Select a predefined `instdata` definition set. This sets the **Active set** indicator. The output layout of the RA options is defined based on the selected definition set.
U	Unselect a selected `instdata` definition set. When no set has the **Active set** indicator, the `instdata` is displayed as is.
I	Insert a new `instdata` definition set to specify mappings and output layouts.
E	Edit an `instdata` definition set to specify mappings and/or output layouts.
D	Delete an `instdata` definition set.

The first time **SETUP Instdata** is selected, or after issuing the **I** (insert) line command, the panel shown in Figure 552 is displayed.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                     zSecure Suite - Setup - Instdata
Command ===> ____________________________________________________________

Enter INSTDATA definition set name for new instdata layout mapping
Name  . . . . . . . . . ________                (INSTDATA definition set)
Description . . . . . . ________________________________  (optional)
```

Figure 552. Setup Instdata- Definition set name

After specifying a unique Instdata definition set name, or after issuing the **E** (edit) line command for an existing set, the Class selection panel is displayed:

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                     zSecure Suite - Setup - Instdata     Row 1 to 4 of 4
Command ===> _____________________________________________ Scroll ===> CSR

Select( S ) the class you want to maintain INSTDATA mapping for

-------------
    Class
S   USER
_   GROUP
_   DATASET
_   RESOURCE
****************************** Bottom of data ********************************
```

Figure 553. Instdata Setup - Class selection panel

The class selection display is used to select the class for which you want to maintain an `instdata` mapping and output layout definitions. When a class is selected (by the **S** line command), the `instdata` mapping definition panel is displayed:

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                     zSecure Suite - Setup - Instdata
Command ===> ____________________________________________________________

Instdata mapping definition
Field name        Default output header          Pos  Len  Format
PHONE             Phone no                       1    10   ________________
ROOM              Room no                        12   5    ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
________________  _____________________________  ___  ___  ________________
Output layout definition
_  Overview display output          _  Detail display output
_  Concise print output             _  Detail print output
_  Concise narrow print output      _  Detail narrow print output
```

Figure 554. Instdata Setup - Mapping definition

You can use this panel to maintain the `instdata` mapping for the selected class.

The following fields are available on this panel:

Table 654. Instdata Setup - Mapping definition field descriptions

Field	Explanation
Field name	The field name. The field name must be unique for the selected class and must not be the same value specified in a predefined field name. This field is required.
Default output header	Specifies the header that is used when no overriding header is specified on the output layout definition panel. When no default output header is specified, the field name is used.
Pos	Indicates the start position of the field within the `instdata`. This field is required.
Len	Indicates the length of the field within the `instdata`. This field is required.

Table 654. Instdata Setup - Mapping definition field descriptions (continued)

Field	Explanation
Format	Specify an output format, HEX or NUM for example. The default output format is CHAR (as it is for `instdata`).
Output layout definition	Select one or more reports to maintain the output layout definition for.

Selecting one or more output layout definitions opens an additional panel so the output layout can be specified.

```
 Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                     zSecure Suite - Setup - Instdata
Command ===> ____________________________________________________________

Output layout definition
Detail display output
N  Field name  P  Header            Len  Output modifiers
   PHONE       /  ________________  10   ____________________________________
/  ROOM        /  ________________  5    ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
_  __________  _  ________________  ___  ____________________________________
```

Figure 555. Instdata Setup - Mapping definition output layout

The following fields are available on this panel:

Table 655. Instdata Setup - Mapping definition output layout field descriptions

Field	Explanation
N	Checkbox that indicates if the field is displayed on a new line. The checkbox is not available for the *display overview* and *concise print output layout* definitions.
Field name	The name of the field to be displayed. The field must have a corresponding definition.
P	This checkbox can be selected to indicate if the field value is prefixed with the header. The checkbox is not available for the *display overview* and *concise print output layout*.
Header	This header for this field. If this value is specified, the value overrides the default output header. When no header is entered, the default output header is used.
Len	The length for this field. If this value is specified, it overrides the default length as specified on the `instdata` mapping definition panel.
Output modifiers	On this field you can enter one or more output modifiers, separated by commas. See "General output modifiers: Controlling field-related output" on page 798 and "Display modifiers: Changing field output display in ISPF" on page 802 for valid output modifiers.

When you exit the Setup Instdata panel and enter `RA.U` option, the detail display shows the `instdata` that you have specified. Figure 556 on page 1665 shows an

example of the panel.

```
zSecure Suite USER overview                                  Line 1 of 66
Command ===> ____________________________________________ Scroll===> CSR
All users                                                 17 Sep 2002 09:20

_ Identification of SYSADM                                           PROD
  User name                    SYSTEM ADMIN
  Phone no                     0152513333
  Room no                      R.103
_ Owner                        SYS1
```

Figure 556. RA.U - Instdata defined for users

SE.7 Setup - Output

You can use the Setup Output option to specify settings for generating output like the page and line length and the printer options. These options affect the P (print) line command on the Results panel. The settings are also reflected in the generated JCL. They have no effect on the behavior of the PRT primary command.

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------
                    zSecure Suite - Setup - Output
Command ===> ____________________________________________

Report options for following runs
Pagelength . . . . _____
Linelength . . . . _____

_  Convert all printed output to uppercase
Print options                      SMTP options
Destination . . .  ________________ SMTP node . . . .  ________
Sysout class  . .  _                SMTP sysout . . .  B
Writer id . . . .  ________         SMTP writer . . .  SMTP
Copies  . . . . .  ___
Character set . .  ____
FCB . . . . . . .  ____
Forms . . . . . .  ____
Output descriptor  ________
Forms overlay . .  ____
```

Figure 557. Setup Output panel

The descriptions for the fields available on this panel are provided in the following list.

Report Options

Pagelength
Sets the page length for use in printable reports. A page length of 0 suppresses all but the first occurrence of the page header and column headers. The maximum value is 32760.

Linelength
Sets the useful line length of the output data sets for later runs. The DCB LRECL value for the data set is set to the value of linelength + 4. The LRECL for the current run is not affected. Information about the output might be lost if the value is too small. The minimum recommended value is 133.

Convert all printed output to uppercase
Specify that all output is to be listed in uppercase, instead of mixed case.

Print options

The Print options fields can be used to specify the (TSO PRINTDS command) options for printed output.

Destination
Specifies the destination to which the output is routed for final processing. The destination is in the form: **destination.userid** or **destination**, where the destination and the userid are 1 - 8 characters. For further information about the TSO PRINTDS command (DEST operand), see the TSO/E Command Reference.

Sysout class
Specifies the JES output class to be used for the output processing of this data set. Default is output class A. For further information about the TSO PRINTDS command (CLASS operand), see the TSO/E Command Reference.

Writer id
Specifies a name for use in processing or selecting a SYSOUT data set. For further information about the TSO PRINTDS command (WRITER operand), see the TSO/E Command Reference.

Copies
Specifies the number of original copies to be printed for the data set. The value for copies can be within the range from 1 to 255. For further information about the TSO PRINTDS command (COPIES operand), see the TSO/E Command Reference.

Character set
Specifies the names of the character arrangement table. For further information about the TSO PRINTDS command (CHARS operand), see the TSO/E Command Reference.

FCB
Specifies the forms control buffer or image used. For further information about the TSO PRINTDS command (FCB operand), see the TSO/E Command Reference.

Forms
Specifies that the output data set is to be printed on a special output form. This value must be from 1 to 4 alphanumeric or national characters. For further information about the TSO PRINTDS command (FORMS operand), see the *TSO/E Command Reference*.

Output descriptor
Specifies a list of output descriptors for the SYSOUT data set. For further information about the TSO PRINTDS command (OUTDES operand), see the *TSO/E Command Reference*.

Forms overlay
Identifies the name of the forms overlay to be used. For further information about the TSO PRINTDS command (FLASH operand), see the *TSO/E Command Reference*.

SMTP options
Ask your system programmer for the correct settings for these options.

SMTP node
Specifies the NJE destination where email is routed for final processing.

SMTP sysout
Specifies the JES output class to be used for the SMTP output processing of emails.

SMTP writer
Specifies a name for use in SMTP selecting an email SYSOUT data set. The external writer name is equal to the SMTP address space name.

SE.8 Setup - Command files

Although all Setup functions can be set individually, the Setup Command files option can apply system-wide or to a group of users, as a suboption under Setup default. See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. When set individually, the SE.8 menu option is equivalent to option `CO.1`. For additional information about the option, see "CO.1 LIBRARIES - Data set selection" on page 1676.

SE.U SETUP - user-defined input sources

This option allows you to define `NEWLIST` types by using `DEFTYPE` (see also "DEFTYPE" on page 777). Actually it allows you to specify a member that contains the `DEFTYPE` and any relevant `DEFINE` statements. When you enter this option initially, the following panel is displayed.

```
         Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                          zSecure Suite - Setup - User defined
Command ===> ____________________________________________________________________

Enter DEFTYPE data definition

Deftype . . . . . . . . ____________________
Description . . . . . . ____________________________________________
Abbreviation  . . . . . __
Data set name(member)   ____________________________________________________
```

Figure 558. Setup user-defined input sources panel

The following fields are available for setting up user-defined input sources:

Deftype
Name of the NEWLIST type.

Description
The description of this type of `NEWLIST`.

Abbreviation
A two character abbreviation for this `NEWLIST`. This abbreviation must be unique for every `NEWLIST` type. It is used for ddname generation.

Data set name(member)
The data set name and member of the define statements.

After all fields are entered, press **`END`**. The results are shown in a table display.

```
        Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                          zSecure Suite - Setup - User defined  Row 10 from 40
Command ===>                                                  Scroll ===> CSR

Select DEFTYPE library ( S (select) E (edit) B (browse) R (repeat) I (insert)
or D (delete))

------------------------------------------------------------------------------
    Deftype                   Description                               Abbr.
Data set name(member)
_   SYSL                      Syslog                                    LG
'YOUR.C2RSAMP(U2RSYSL)'
------------------------------------------------------------------------------
```

Figure 559. Setup user-defined input sources - Deftype definitions table

The same table is displayed when you enter SE.U after you have created your first user-defined input source. Table 656 lists the line commands available for user-defined input sources.

Table 656. User-defined input sources - available line commands

Command	Description
S	Select set to view or edit definition.
E	Edit the specified member.
B	Browse the specified member.
R	Repeat DEFTYPEdefinition.
I	Insert new DEFTYPE definition.
D	Delete this line.

Input sources for this user defined NEWLIST type can be specified with Setup Files.

SE.C SETUP - Change track

Use the Change Track option to monitor system and security attributes that you specify.

Figure 560 shows the Setup Change Track menu.

```
Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                    zSecure Suite - Setup Change Track
Option ===> ____________________________________________________________

D    Data sets       Maintain list of sensitive data sets
M    Site msgs       Site defined message table
C    zSecure msgs    zSecure defined message table
```

Figure 560. Setup Change Track panel

Table 657 describes the options available from this menu.

Table 657. Setup Change Track menu options

Change track option	Descriptions
D	Manage data sets your site considers sensitive. See “SETUP - Change Track Data Sets” on page 1669.

Table 657. Setup Change Track menu options (continued)

Change track option	Descriptions
M	Manage your site defined messages. See "SETUP - Change Track messages" on page 1670.
C	When you select this option a panel opens for browsing the messages defined by zSecure.

SETUP - Change Track Data Sets

By default, the Change Tracking system monitors changes to the protection of all data sets considered sensitive by REPORT SENSITIVE. In addition to these you can mark additional data sets as sensitive using SETUP - Change Track Data sets.

On entry to this option a list of sensitive data sets is displayed:

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                       zSecure Suite - Change Track Sens Row 1 to 2 of 2
Command ===> _____________________________________________ Scroll===> CSR

Insert, Delete or Select (I/D/S) a data set mask

     Data set mask                                  Access   System
                                                    level
     SYSAPP.**                                      UPDATE   CR#4
     SYS1.**                                        READ     *
****************************** Bottom of data ********************************
```

Figure 561. Setup Change Track - sensitive data sets

The first time you enter this option the list will be empty. You can add entries using the **I** line command:

```
 Menu   Options   Info   Commands
------------------------------------------------------------------------------
                       zSecure Suite - Change Track Sens Row 1 to 2 of 2
Command ===> _____________________________________________ Scroll===> CSR

Data set mask                                 Access   System
SYSAPP.DATA.**_____________________________ READ____ CR#4_________________
Reason Confidential application data sets_____________________________________
```

Figure 562. Setup Change Track - initial view of sensitive data sets panel

To mark a data set, or a group of data sets, as sensitive, the following fields must be defined:

Data set mask
An EGN mask matching the data sets that you consider sensitive.

Access
The level of access that you want to report on. For integrity-sensitive data sets, set the Access level to UPDATE. For confidentiality-ensitive data sets, set the access level to READ.

System
The SYSNAME of the system where these data sets are considered sensitive. If the data sets are sensitive on all your monitored systems, you can use an '*'.

Reason
This is a comment field to document why these data sets have been marked sensitive.

After specifying the desired settings, pressing ENTER to add the data sets to the list of sensitive data sets and return to the initial display.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Change Track Sens Row 1 to 3 of 3
Command ===> _____________________________________________ Scroll===> CSR

Insert, Delete or Select (I/D/S) a data set mask

      Data set mask                                    Access   System
                                                       level
      SYSAPP.**                                        UPDATE   CR#4
      SYSAPP.DATA.**                                   READ     CR#4
      SYS1.**                                          READ     *
****************************** Bottom of data ********************************
```

Figure 563. Setup Change Track - list of sensitive data sets

The **D** action character can be used to remove a data set mask from the list. The **S** action command will display the sensitivity reason.

SETUP - Change Track messages

Use the Setup Change Track Messages option to maintain message IDs to be used with the Change Tracking system (AU.C). Each type of system change is associated with its own associated message ID. For example, message ID U000001 can be defined to represent the addition or deletion of a page data set. These messages use the following message prefix conventions to categorize messages by type.

- **U** indicates a site-defined message.
- **C** indicates a product message that cannot be changed.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Site message table     Row 1 to 1 of 1
Command ===> _____________________________________________  Scroll===> CSR

Insert, Delete, Edit or Browse (I/D/E/B) a message id

   Message Number  Message Description
   U000001         MVS IPL page datasets
****************************** Bottom of data ********************************
```

Figure 564. Setup Change Track - Site message table

Table 658 describes the line commands for the Site message table.

Table 658. Setup Change Track - available line commands for the Site message table

Command	Description
I	Insert a new message id. This command allows you to monitor for changes that have not been predefined.
E	Edit the message id. This command can be used to change what is monitored or displayed by Change Tracking.
D	Delete a message id. After this command runs, the event that the message id describes is no longer tracked.

Table 658. Setup Change Track - available line commands for the Site message table (continued)

Command	Description
B	Browse the message id This can be used to see what is monitored or displayed by Change Tracking.

When you edit, browse or insert a Message id, the Message ID specification panel shown in Figure 565 opens for viewing, modifying, or specifying the message ID settings.

```
 Menu   Options   Info   Commands
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Change  Row 1 to 22 of 31
Command ===> ____________________________________________________________

Message id  . . . . . . U210001
Message description . . System special
Action on addition  . . ALU userid NOSPECIAL to remove attribute
Action on delete  . . . ALU userid SPECIAL to re-instate attribute

Flags:
Deletes reported    YES  Additions reported  YES
Confirm allowed     YES  Reject allowed      YES

Enter NEWLIST type and CARLa define/select statements
NEWLIST type RACF
Define . . .
Select . . . CLASS=USER SEGMENT=BASE SPECIAL
****************************** Bottom of data ********************************
```

Figure 565. Setup Change Track - Site message detail view

The following fields are available to define or change a site message definition:

Message id
The ID (between U000001 and U999999) assigned to this type of change. The message ID must be unique.

Message description
Describes this type of change. The value is shown in the Change Tracking system.

Action on addition
Determines the appropriate action to take if the change is an addition and has not been approved.

Action on deletion
Determines the appropriate action to take if the change is a deletion and has not been approved.

Deletes reported
Determines if delete operations are reported for this attribute. Select YES or NO.

Additions reported
Determines if add operations are reported for this attribute. Select YES or NO.

Confirm allowed
Determines if users of the Change Tracking system are permitted to confirm this change. Select YES or NO.

Reject allowed
Determines if users of the Change Tracking system are permitted to reject this change. Select YES or NO.

newlist type
The NEWLIST type for reporting this change. You can specify any of the following types: AUTAB, CLASS, RACF, ROUTER, RRNG, SPT, TEMPLATE, CONSOLE, DASDVOL, DSNT, EXIT, IOAPP, JOBCLASS, MSG, PC, PPT, SENSDSN, SMFOPT, SUBSYS, SVC, or SYSTEM.

Define
Specify one CARLa define statement for both the selection and list operations. You only need to enter the define clauses, not the word *Define* itself.

Select
Specify one CARLa select statement to identify what you want to monitor. Selection fields must be valid for the NEWLIST type you specified earlier. You only need to enter the define clauses, not the word *Define* itself.

After you enter the message definition information, the panel shown in Figure 566 opens.

```
  Menu   Options   Info   Commands
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Change  Row 1 to 31 of 31
Command ===> ____________________________________________________________

Enter fields, field lengths and descriptions to report
Fieldname               Length  Description
KEY                     8       Userid




****************************** Bottom of data ********************************
```

Figure 566. Setup Change Track - Site message reporting options

On this panel, you can specify the information in the message to include in the reports like the profile name or user name for example. Always specify the name values so that the details reported uniquely describe the change you are tracking. The following fields are available:

Field
Specifies the field name. You can use any of the valid field names for the NEWLIST type you specified as long as the field is not part of a repeat group.

Length
The output length of the field.

Description
Specifies the field description that is provided on the Change Tracking detail display.

The **SE.C.C** menu option for messages defined in zSecure shows a similar display panel. However, the only action command permitted is **B** (browse).

SE.N Setup - National Language Support

Although all Setup functions can be set individually, the Setup - National Language Support files option can apply system-wide or to a group of users, as a suboption under Setup default. See *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

SE.T Setup - Trace

Use Setup Trace for configuring the product to provide a trace. Most options are created for debugging and diagnostics. Consequently, they are turned off unless you are trying to diagnose a problem. Typically, you do not need to configure these options unless you are asked to do so by IBM software support. If you select the Trace command, these options can cause errors and unexpected results.

Figure 567 shows the Setup - Trace menu options panel that opens when you select the Setup Trace option from the Setup menu.

```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                     zSecure Suite - Setup -  Trace
Command ===> ____________________________________________________________

Diagnose syntax errors or enhance your CARLa knowledge
  /  List standard CARLa members


Use following options only at the direction of IBM sofware support
 Enter "/" to select option(s)
  _  Show parameters in run
  _  Show intermediate results during recursion
  _  Show ISPF dialog errors (if selected some parts may fail)
  _  Trace REXX programs
  _  Trace ISPF panel processing (z/OS 1.7 and up)
  _  Trace ISPF skeleton processing (z/OS 1.7 and up)
  _  Pass abends to ISPF
  _  Prevent closing/freeing data sets during abend recovery
  _  Suppress error traps (if selected some parts may fail)
  _  Debug action commands
  _  Show CKGRACF command flow
  _ Collect CKX diagnostic information
```

Figure 567. Setup Trace panel

Descriptions for the available Setup Trace options are provided in the following list.

List standard CARLa members
If this option is checked, all included members are shown expanded in the SYSPRINT file. The expanded view can be helpful for understanding the query sent to the product engine by the interface. This option is useful when you are developing or learning about CARLa programs.

Show parameters in run
If this option is checked, a panel opens to show the parameters passed to the program.

Show intermediate results during recursion
If this option is checked, commands generated during a recursive run are immediately displayed in BROWSE mode. Normally, the commands are presented after finishing the run.

Show ISPF dialog errors (if selected some parts may fail)
If this option is checked, the ISPF RETURN error mode is set (`CONTROL ERRORS RETURN`). Some parts of the interface might fail when this option is selected.

Trace REXX programs
If this option is selected, the panel shown in Figure 568 on page 1674 opens so you can set a specific REXX Trace option.

```
 Menu  Options  Info  Commands  Setup
_____________________________________________________________________________
                        zSecure Suite - Setup - Trace Rexx
Command ===> _____________________________________________________________

Select one of the following Rexx Trace options, or blank to disable tracing:
_  1. All            Traces all clauses before execution
   2. Commands       Traces all commands before execution
   3. Error          Traces any command resulting in an error or failure
   4. Intermediates  Traces all clauses and intermediate results
   5. Labels         Traces only labels passed during execution
   6. Normal         Traces any command resulting in a negative return code
   7. Results        Traces all clauses before execution and final results
```

Figure 568. Setup Trace REXX options

The selected Trace option is effective for all the zSecure REXX programs. For further information about the different Trace options, see the "TSO/E REXX reference".

Trace ISPF panel processing (z/OS 1.7 and up)
If this option is checked, a panel trace is activated using the ISPDPTRC command. After leaving the user interface, the output of the panel trace is displayed in VIEW mode.

This option is only available on z/OS 1.7 and up. Only use this option at the request of IBM software support in order to diagnose panel processing problems.

For further information about the ISPDPTRC command, see the IBM manual *ISPF Dialog Developer's Guide*.

Trace ISPF skeleton processing (z/OS 1.7 and up)
If this option is checked, a skeleton trace is activated using he ISPFTTRC command. After leaving the user interface, the output of the skeleton trace is displayed in VIEW mode.

This option is only available on z/OS 1.7 and up. Only use this option at the request of IBM software support in order to diagnose skeleton processing problems.

For further information about the ISPFTTRC command, see the IBM manual *ISPF Dialog Developer's Guide*

Pass abends to ISPF
If this option is checked, the NOCLEANUP parameter is added to the CARLa ALLOC command. This option can be used for debugging purposes to pass on abends to ISPF instead of recovering from them. Only use this option at the request of IBM software support when an attempt to cleanup the abend causes additional errors.

Prevent closing/freeing data sets during abend recovery
If this option is checked, the NOCLOSE parameter is added to the CARLa ALLOC command. This option can be used to prevent closing and freeing data sets during abend recovery processing. Only use this option at the request of IBM software support.

Suppress error traps (if selected some parts may fail)
Suppresses error traps during a debugging session. If this option is checked, the NOESTAE parameter is added to the CARLa ALLOC command. Setting this option can cause the product to stop working.

Debug action commands
Enables tracing of the authority checks made to decide which items are shown

on menus and which actions characters are available to the user. The trace is written to the C2RIMENU ddname and can be viewed using the C2RIMENU primary command. The option also enables tracing of action character processing by adding message CKR2829 in the SYSPRINT. The latter effect can also be achieved in user-defined queries by adding the CARLa command DEBUG ACTION.

Show CKGRACF command flow
If this option is checked, the CKGRACF DEBUG command is issued with some additional parameters before every CKGRACF command. The CKGRACF DEBUG command is designed to explore how CKGRACF operates or to diagnose problems in its operation. This option is especially helpful in determining why a certain CKGRACF command is not allowed.

Collect CKX diagnostic information
Enables collection of CKX diagnostic information. The information is written to the CKXDEBUG ddname and can be viewed using the CKXDEBUG primary command.

SE.W SETUP - Windows

Use the Setup Windows option for configuring zSecure Visual, the Microsoft Windows client for IBM Security zSecure Admin. This option is only available when zSecure Visual is installed and not disabled in IFAPRDxx. When you select SE.W, the panel shown in Figure 569 opens.

```
Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                          zSecure Visual - Configuration
Command ===> ____________________________________________________   _ start panel

 1  1. Add, delete, or install zSecure Visual Windows client

Server  . . . . . . IPO1                                          (IP or DNS)
Server base port  . 8000                                 (IP base port of server)

Act Agent id         IP number or DNS name                         Port (opt.)
AP  12.1. 100_______ CRM100_____________________________________ __________




Act must be A, D, P, C, AP (A=add D=delete C=cancel pwd P=new pwd)
```

Figure 569. zSecure Visual - Configuration

For additional information about configuring the zSecure Visual client, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

SE.D SETUP - Default

Use the Setup Default option for configuring installation-wide default settings. For more information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

SE.R Setup - Reset to system default

Use the Setup Reset option to reset your settings to the system default values. The default settings are copied over your settings. Your personal sets of input files remain unchanged, only the system-defined sets are replaced by the new sets.

SE.I Setup - Installation

Although all Setup functions can be set individually, the Setup Installation option can be used to set system-wide options or options for user groups. It is a suboption of the Setup Default option. For more information, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

CO Commands - Run Commands from Library

The LIBRARY application is always available as option **CO** from the main menu. It lets you manage your own libraries of commands, or run CARLa queries supplied with the product. The panel is organized from top to bottom to use: data sets (**1**), member list (**2**), specific members (**3**-**5**), and commands stored in ISPF profile (**C**).

```
 Menu  Options  Info  Commands  Setup          StartPanel
--------------------------------------------------------------------------------
                      zSecure Suite - Commands
Option ===> ____________________________________________________________

 1      Libraries       Select and maintain command library
 2      Members         Work with members from current command library
 3      Edit            Edit member from current command library
 4      Run             Run member from current command library
 5      Submit          Run member from current command library in background
 C      Command         Type in any CARLa command



 Member name . . . . ________      (If 3, 4 or 5 selected)
 Two pass query  . . N             (Y/N, option 4 only)
 Current library . . DD:CKRCARLA
 Input complex . . . Control blocks in common storage and live SMF datasets
 Current mask type . EGN
```

Figure 570. Commands menu

The next pages describe the options **1**, **2** and **C**. Options **3** to **5** operate directly on the member entered on the panel. Option **Two pass** query is only applicable for option **4**. Select `Y` when it is a two-pass query and no customization is necessary.

CO.1 LIBRARIES - Data set selection

Option **CO.1** allows you to allocate and select an existing library for subsequent use. The initial contents of this option is the system default set as described in *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. If no default is specified, this setting contains only DD:CKRCARLA, the ddname for the default CARLa library. You can use the I line command to insert new libraries. To activate a library use the `S` line command.

```
 Menu   Options   Info   Commands
--------------------------------------------------------------------------------
                       zSecure Suite - Setup - Command file Row 1 from 3
Command ===> ____________________________________________ Scroll ===> CSR

Select CARLa script library or work with a library (E, R, I, or D)

   CARLa script library
_  DD:CKRCARLA                                                      default
****************************** Bottom of data ********************************
```

Figure 571. Setup - Command file panel

Each line in the library selection list must contain a data set name using TSO conventions, or DD: followed by an allocated filename. The library marked **selected** is used by the other options of the COMMANDS menu.

The following line commands can be used to select libraries.

E	Show the members in this library
D	Delete the line from the selection list, the data set is **not** deleted
I	Insert an empty line following this line, it is not selected automatically
R	Repeat name in this line
S	Select the library for subsequent use

When you have selected a data set, you can call up a member list of the data set with the E line command, or exit the library selection panel and use option **CO.2**.

CO.2 MEMBERS - Member selection

You can use the member selection panel to select a member for edit or to invoke the program in the foreground or in the background with the selected member as input.

```
LIBRARY          C##A.D.C##NEW.SCKRCARL                  Row 00001 of 00008
Command ===> _____________________________________________ Scroll ===> CSR
Valid line commands are B(browse), E(edit), J(job) and R(run in foreground)
   Name     Prompt          Size    Created          Changed          ID
. CKRL$ALL                   27   1998/03/10   1998/03/10 14:16:11   RCR2300
. C2RL$UNL                   25   1997/05/16   2000/06/19 18:04:06   RCR2600
. CKRLAC1                    66   1998/02/12   2001/09/17 17:19:03   C##ASCH
. CKRLAPPL                   24   1998/02/12   1998/02/12 15:19:27   RCR2300
. CKRLAUD                    36   1997/02/24   1997/02/24 12:15:45   RCR2200
. CKRLAUTH                   66   1998/02/12   2001/09/17 17:27:10   C##ASCH
. CKRLCICS                  133   1998/02/12   1998/02/12 15:19:52   RCR2300
. CKRLCICT                   32   1998/02/12   1998/02/12 15:19:01   RCR2300
```

Figure 572. Command Library - Member selection panel

The member selection list supports the following primary commands:

```
EDIT member
SELECT member
LOCATE member
SORT column
```

You can abbreviate the Edit and Select keywords as `E` and `S`, respectively. The `Member` can be a new or an existing member name, or a pattern with an asterisk. For example, to limit the list to members that start with *`CKRL`*, you can enter *`S CKRL*`*.

Table 659 lists the commands for selecting members.

Table 659. Command Library Member selection line commands

B	Browse a member
E	Edit a member
J	Submit a job with the member as input
R	Run the program in the foreground using the member as input
S	An alias for E

For information about the commands for editing a member, see “Primary commands” on page 11.

CO.C COMMAND - Type in any CARLa Command

Use Option **CO.C** to run CARLa (CARLa Auditing and Reporting Language) commands and view the output. (See Chapter 12, “CARLa Command Language,” on page 713 for CARLa command documentation.) The commands you enter are saved in the ISPF profile data set for later reference. After the commands complete, you are presented with the report file if present, or with the message file if no report is produced.

- Run a CARLa command and view the output.
- Save the command input for later use.

Commands can be entered using the ISPF editor. The editor opens the current library, SCKRCARL, for example and uses a member name that consists of a number sign (#) followed by your userid. If such a member exists in the library, the content is not used, nor is it destroyed when you leave the editor. Enter SAVE to save the commands in the ISPF profile, enter CANCEL to leave the editor without saving the contents. Figure 573 shows the panel for entering the commands.

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
EDIT ---- C##.C2R113.SCKRCARL(#USERID)  - 01.00              Columns 00001 00080
Command ===> _____________________________________________ Scroll ===> CSR
****** ***************************** Top of Data ******************************
=NOTE= Enter GO or RUN to execute commands, SUB or SUBMIT to generate batch job
=NOTE= END or SAVE to save in ISPF profile
''''''
''''''
''''''
''''''
''''''
''''''
''''''
''''''
''''''
''''''
''''''
****** **************************** Bottom of Data ****************************
```

Figure 573. Command input panel

When you enter GO or RUN on the command line, the commands in the editor are executed by Security zSecure, at your terminal. When you enter SUB or SUBMIT, a batch job is generated to run the commands, with the same options and input files that your current ISPF session uses.

The primary command CARLa directly invokes this option.

An introduction to CARLa

The following sections give some examples of the use of the LIST and SORTLIST commands, optionally together with SELECT parameters. The LIST and SORTLIST commands can be used to In addition, multiple custom reports can be generated using the NEWLIST command.

Use LIST and SORTLIST commands to create customized reports for RACF profile information.

Use the NEWLIST command to generate multiple custom reports.

Use SELECT and EXCLUDE commands to select the records and information to be included in the report.

If no SELECT/EXCLUDE is given, all profiles are selected by default. The advantage of NEWLIST is that each custom report can have its own selection statements.

Listing profile fields

Use the following CARLa commands to select and list the profile fields to include in a custom report or ISPF display.

- LIST
- SORTLIST
- DISPLAY
- SUMMARY

The parameters of these commands are field names. Field names can include the following value types:

- Values defined by Security zSecure such as CLASS and KEY
- Built-in alias names defined for commonly used flags like SPECIAL.
- Field names defined in the RACF database *templates*.

The templates can be displayed using the `SHOW TEMPLATE` command, or by running the TEMPLATE command from the Security zSecure command line. Sample templates are listed in "TEMPLATE - Template field properties" on page 284. A reference of the field names available is included in "RACF: RACF profiles" on page 1124.

As an example, the code to list profile class, name, and standard access list:

```
SORTLIST CLASS KEY USERID USERACS
```

This query might for example give the following output (REPORT file and SYSPRINT file, only relevant parts are displayed).

```
Include CKRALLOC (ISPF variable)
     2 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.CKFREEZE'  complex=DINO rrsfnode=THESRRSF
     3 |
     5 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.UNLOAD'  complex=DINO rrsfnode=THESRRSF
     6 |
     8 |/* Daily Backup */
     9 |alloc type=CKRCMD DD=CKR2CMD complex=DINO
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
     1 |sortlist class key userid useracs
End of  CKRCMDV  (include level 1)

P R O F I L E   L I S T I N G   30 May 2007 00:07                                                    Page 1

Class    Profile key                              User/grp Access
ACCTNUM  **                                       IBMUSER  ALTER
                                                  C##A     READ

DATASET  ADM1.**
DATASET  ADM1.SPECIAL.*
DATASET  ADM1.SPECIAL.*.**
DATASET  ADM1.SPECIAL.**
FACILITY $C2R.SERVER.ADMIN                        C##CWGS  READ
                                                  S##PROG  READ
                                                  C##ADMIN READ
GROUP    ADMIN                                    FIN1     USE
                                                  ADM1     USE
                                                  ADM2     USE
                                                  FIN2     USE
GROUP    DLIBR9
GROUP    NONEXI2
               NONEXI2U USE
JESSPOOL &RACLNDE.DSNASTC.**                      D##ADBA  READ
                                                  S##PROG  ALTER

STARTED  ANTAS000.*
STARTED  CONSOLE.*
STARTED  CONSOLE.*                                C##BMR1  ALTER
STARTED  DLF.*
STARTED  DLF.*                                    C##BMR1  ALTER
STARTED  DSN1*.*
STARTED  DSN1*.*                                  C##BMR1  ALTER
STARTED  DSN1*.**                                 C##BMR1  ALTER
                                                  C##BGUS  ALTER

STARTED  DSN1MSTR.*
STARTED  DSN1MSTR.*                               C##BMR1  ALTER
                                                  C##BGUS  ALTER

STARTED  DUMPDASD.*
STARTED  DUMPDASD.*                               C##BMR1  ALTER
STARTED  EPWFFST.*
STARTED  EPWFFST.*                                C##BMR1  ALTER
UNIXMAP  U2                                       S##TS20  NONE
                                                  S##TS19  NONE
                                                  C##BMR3  NONE
```

Figure 574. Sample SORTLIST output with access list - SYSPRINT and REPORT files

Generally, issuing the SORTLIST or LIST command generates more output than you want. The results of these commands include at least one line for each segment for each profile in the database if the database is in Restructured Data Set format. You can use the SELECT command to define selection criteria to limit the profiles included in the results. For instance:

```
SELECT CLASS=DATASET SEGMENT=BASE
SORTLIST CLASS KEY USERID USERACS
```

Sample output for this function:

```
P R O F I L E   L I S T I N G   12 Oct 2001 00:07                                                    Page 1

Class    Profile key                              User/grp Access
DATASET  ADM1.**
DATASET  ADM1.SPECIAL.*
DATASET  ADM1.SPECIAL.*.**
DATASET  ADM1.SPECIAL.**
```

Figure 575. Sample SORTLIST output with access list - DATASET profiles

The width of each column is derived from the templates and from an internal table. You can modify this width by giving the length in parentheses. For example, since you know that for the GLOBAL class, the profile name is a RACF class, and class names are not longer than 8 characters, you can issue the following CARLa commands:

```
SELECT CLASS=GLOBAL
SORTLIST CLASS KEY(8) MEMLST
```

These statements print all GLOBAL profiles with their member profiles as shown in Figure 576 on page 1681. zSecure automatically formats the option bytes in the

members. For GLOBAL profiles, it is the universal access.

```
P R O F I L E   L I S T I N G   12 Oct 2001 00:07                                                    page    1

Class    Profile  Members
GLOBAL   DATASET  SYSS.*.ISPCLIB.VB/READ
                  SYSS.*.ISP%LIB/READ
                  C##BERT.C##QA%%%.*/READ
                  &RACUID.*.**/ALTER
                  SYS1.PP.ISP*.**/READ
GLOBAL   JESJOBS  SUBMIT.&RACLNDE.&RACUID%.&RACUID/READ
GLOBAL   JESSPOOL &RACLNDE.*.&RACUID*.*/ALTER
```

Figure 576. Sample SORTLIST output with explicit length

The major LIST, SORTLIST, and DISPLAY commands each behave differently in terms of the sequence of the profile listing and in the use of main memory.

- The LIST command outputs the profiles in the order as present in the RACF database or unloaded input file.

  The SORTLIST and DISPLAY commands sort the profiles in ascending order according to the sequence of field names on the command.
- The LIST command does not store the profiles in main memory.

  The SORTLIST and DISPLAY commands store and sort the profiles in main memory.

The LIST command is therefore more suited to tasks requiring further postprocessing by computer, while SORTLIST and DISPLAY are ideal for making reports and displays based on the selected field names.

The following command shows an example of the standard CKRLPROG member supplied in the SCKRCARL data set, combining the commands discussed before.

```
Include CKRALLOC (ISPF variable)
     2 |/* Data for CKRLPROG */
     3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD971028.UNLOAD'  complex=DD971028
     4 |
     6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD971028.CKFREEZE'  complex=DD971028
     7 |
     8 |alloc type=CKRCMD DD=CKR2CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
     1 |I DD=CKR2CRL M=CKRLPROG

Include CKR2CRL  C##A.D.C2RNEW.SCKRCARL(CKRLPROG)                       SM3005
     1 | /*************************************************BeginModule********
     2* | * LICENSED MATERIALS - PROPERTY OF IBM
     3* | * 5655-T01
     4* | * Copyright IBM Corp. 1989, 2007
     5* | * All Rights Reserved
     6* | * US Government Users Restricted Rights - Use, duplication or
     7* | * disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
     8* | * File-stamp: <020404 MR 11:37:08 CKRLPROG.SCKRCARL>
     9* | * FMID: HCKR181 RMID: HCKR181 IBM Security zSecure Base 1.9.0
    10* | * Purpose:
    11* | *     Program Profile Overview
    12* | *     Program Accessed Dataset Overview
    13* | * History:
    14* | ************************************************EndModule********/
    15 |newlist title='Program profile overview'
    16 |   select   class=program segment=base
    17 |   sortlist key(nondispl) | complex key(8) memlst(sort) uacc(3),
    18 |                  acl(sort,43) acl:pgmrname
    19 |
    20 |newlist title='Program Accessed Dataset overview'
    21 |   select   pads class=dataset segment=base
    22 |   sortlist hexkey(nondispl) | complex key(36,wrap) volser dstype uacc,
    23 |                       acl(sort,43) acl:pgmrname
    24 |
End of  CKR2CRL  (include level 2)

End of  CKRCMDV  (include level 1)
```

Figure 577. Sample output from the CARLa script CKRLPROG (first page only) - Part 1

```
P R O F I L E   L I S T I N G   28 Oct 1997 00:05                                                                  page   1
Program profile overview

Complex  Profile  Members                                                UAC User     Access  ACL id   When             Name
DD971028 *        C##A.I.ISPLLIB/SME003/NOPADCHK                         REA
                  IPO1.LINKLIB//NOPADCHK
                  ISF.V1R5M0.SISFLOAD/M95DR2/NOPADCHK
                  ISP.V4R2M0.SISPLOAD/M95DR2/NOPADCHK
                  SYS1.CMDLIB/******/NOPADCHK
                  SYS1.CSSLIB/******/NOPADCHK
                  SYS1.LINKLIB/******/NOPADCHK
                  SYS1.MIGLIB/******/NOPADCHK
                  SYS1.NUCLEUS/******/NOPADCHK
                  SYS1.PP.ISPLLIB/M95DR2/NOPADCHK
                  SYS1.PPLIB/M95DR2/NOPADCHK
                  SYS1.SCBDHENU/******/NOPADCHK
                  SYS1.SCEERUN/******/NOPADCHK
                  SYS1.SIMWMOD1/******/NOPADCHK
                  SYS1.SISFLOAD/******/NOPADCHK
                  SYS1.SISPLOAD/******/NOPADCHK
DD971028 **       SYS1.NO.DATASET/SMS001/NOPADCHK                        NON R##SLIN  ALTER   R##SLIN                  BERT
DD971028 ABEND806 ETSTROB.R##PROB.DATASET.DOESNOT.EXIST/DISK10/PADCHK    NON C##BERT  ALTER   C##BERT                  BERT
                  SYS1.LINKLIB/M92070/PADCHK
DD971028 ASMIDFA  SYS1.CRM.LINKLIB//NOPADCHK                             NON -group-  READ    S##PROG
                                                                             C##ASCH  READ    C##ASCH                  H SCH
                                                                             C##BABE  READ    C##BABE                  ABE K
                                                                             C##BAB2  READ    C##BAB2                  ABE K
                                                                             C##BGU2  READ    C##BGU2                  GUUS
                                                                             C##BHVN  READ    C##BHVN                  HANS
                                                                             C##BMCO  READ    C##BMCO                  MATTH
DD971028 BERT     MY.DATA0//NOPADCHK                                     NON R##SLIN  ALTER   R##SLIN                  BERT
                  MY.DATA1/B/NOPADCHK
                  MY.DATA2/BR/PADCHK
                  MY.DATA3/BRT/PADCHK
                  MY.DATA4/BERT/PADCHK
                  NOWHERE.TO.BE.FOUND//PADCHK
DD971028 BPXBINIT SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXEV003 SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXOLVD  SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXOV    SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXPLPKA SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXUCSNM SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXUEYI1 SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXUI1EY SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 BPXZ24   SYS1.LINKLIB/******/NOPADCHK                            REA R##SLIN  ALTER   R##SLIN                  BERT
DD971028 CNA*     CRMA.C##PROD.LOAD/SME005/PADCHK                        NON -group-  READ    C##A
                  CRMA.D.CNRNEW.CNRLOAD/CRM001/PADCHK                        -group-  READ    C##ARACF
                  CRMA.D.CNR23B.CNRLOAD//PADCHK                              -group-  READ    C##B
                  CRMA.T.CNR210.CNRLOAD/SME001/PADCHK                        -group-  READ    C##BRACF
                  CRMA.T.CNR211.CNRLOAD/SME002/PADCHK                        -group-  READ    C##C
                  CRMA.T.CNR211.PR60513.CNRLOAD/SME005/PADCHK                -group-  READ    C##CDEMO
                  CRMA.T.CNR211.SRVC.CNRLOAD/SME001/PADCHK                   -group-  READ    C##GRACF
                  CRMA.T.CNR220.BASE.CNRLOAD/SMK001/PADCHK                   -group-  READ    C##QA
                  CRMA.T.CNR221.CNRLOAD//PADCHK                              -group-  READ    S##APPL
                  CRMA.T.CNR221.PR70710.CNRLOAD//PADCHK                      -group-  ALTER   S##PROG
                  CRMA.T.CNR221.PR70809.CNRLOAD//PADCHK                      C##AINT  ALTER   C##AINT                  CONSU
```

Figure 578. Sample output from the CARLa script CKRLPROG (first page only) - Part 2

In the SYSPRINT file shown in the preceding figure, we see that the query specified in the interface (ISPF variable CKRCMDV) was in this case

```
I DD=CKR2CRL M=CKRLPROG
```

which resulted in the inclusion of the CARLa script CKRLPROG from the CKRCARLA ddname (as listed for DDname CKR2CRL—apparently this was a run from ISPF logical screen 2). The CKRLPROG script contains some comments (between "/*" and "*/" pairs) and two separate queries, each starting with a NEWLIST command; the NEWLIST command serves to separate queries as well as to define certain attributes for the report generated by the (following) query, in this case the TITLE to be printed above each page. The first query consists of a SELECT command and a SORTLIST command. The SORTLIST command includes a nondisplay column KEY up front (this column does not result in any output, but it does determine the primary sort order); because of the '|' modifier, the column separator normally printed before a second column is suppressed. The member list (MEMLST) is internally sorted before being printed because of the SORT repeated field modifier. The Universal ACCess level is also printed, truncated to three characters, as is the ACcess List (which results in several columns), and finally ACL:PGMRNAME is a lookup(:) of the user name (PGMRNAME), being done based on the ids on the Access list (to print the user name next to the userid). Only the first page of output of the first query is shown; the output of the second query is not visible.

Finding specific profile field contents

To search for profiles with a specific value in some profile variable field (not a flag field), you can use the general field-value selection mechanism.

Note: Flag fields all have distinct SELECT keywords for the flags. See "Finding profiles with specific attributes" on page 1684).

Generally, a field-value selection can be made with the following command:

```
SELECT fieldname=fieldvalue
```

Note: Flag fields all have distinct SELECT keywords for the flags - see "Finding profiles with specific attributes" on page 1684).

In this statement, the *fieldname* must be the name of the profile field as present in the templates in the RACF database. For a listing of these names, see the IBM RACF manual *Macros and Interfaces*. You can use the command in a batch program or type TEMPLATE on any ISPF panel to obtain a listing of the field names that are defined in your database. "TEMPLATE - Template field properties" on page 284 contains sample output of this command.

The value *fieldname* must be in a format consistent with the type of the field. For example, an access level can have values such as *READ* and *UPDATE*. If the value contains a generic character `%` or `*`, the value is used as a filter where `%` matches one character and `*` matches a qualifier (all characters up to `.` (a period). If the value starts with `:` (a colon), the field is scanned for a substring.

Table 660 list the values supported by the operator field.

Table 660. Profile field - supported operators

Operator	Description
=	Equal
<	Less than
>	Greater than
<=	Less than or equal
>=	Greater than or equal
<>	Not equal
¬=	Not equal

For values that indicate a filter, only equality and inequality operators are supported.

For example, to select data sets with a universal access greater than or equal to UPDATE, you might give the following commands:

```
SELECT CLASS=DATASET, UACC>=UPDATE
SORTLIST CLASS, KEY, UACC
```

Figure 579 on page 1684 gives an example of the output.

```
P R O F I L E   L I S T I N G   28 Oct 1997 00:05                                page 1

Class    Profile key                              UACC
DATASET  CATALOG.UCAT.**                          UPDATE
DATASET  R##PROB.TEST10                           UPDATE
DATASET  SYS1.BRODCAST                            UPDATE
DATASET  USERCAT.**                               UPDATE
```

Figure 579. Sample SELECT with field value selection

You can also search for date fields in profiles. To find all TSO users who have never logged on, or users who have not changed their password, use the following code:

```
SELECT CLASS=USER, S=BASE
NEWLIST TITLE='never logged on'
  SELECT LJTIME='FFFFFFFF'X
  SORTLIST KEY(8) PGMRNAME DFLTGRP OWNER DEFDATE
NEWLIST TITLE='password unchanged for 90 days'
  SELECT PASSDATE<DUMPDATE-90
  SORTLIST KEY(8) PGMRNAME DFLTGRP OWNER DEFDATE PASSDATE
```

You can review the full program for this query in the CARLa scripts CKRLLGNU for the List Logon Never Used report and CKRDLGNU for the List Logon Never Used display output.

The following CARLa statements show an example of scanning for owner fields starting with *SYS*:

```
SELECT CLASS=DATASET OWNER=SYS*
SORTLIST CLASS KEY OWNER
```

The following CARLa statements show an example of scanning for user names containing a substring JONES or SMITH:

```
SELECT CLASS=USER NAME=:(JONES,SMITH)
SORTLIST CLASS KEY(8) NAME
```

Finding profiles with specific attributes

The RACF database can be scanned for users with specific attributes using keywords on the SELECT command. This scanning cannot easily be done easily using the field-value selection described in “Finding specific profile field contents” on page 1683 because the attributes are flags in flag bytes. The SELECT command aims to provide two keyword parameters for each attribute (flag): one for selection if the flag is on, and one for selection if the flag is off. For example, to find users with the UAUDIT (user-audit) attribute, use the following CARLa commands:

```
SELECT CLASS=USER UAUDIT
LIST CLASS KEY
```

To find users *without* the UAUDIT attribute, use the following CARLa commands:

```
SELECT CLASS=USER NOUAUDIT
LIST CLASS KEY
```

To find users with group-SPECIAL attribute, use the following CARLa command:

```
SELECT CLASS=USER GRPSPECIAL
```

To select system-wide and group-special users:

```
SELECT SPECIAL OR GRPSPECIAL
```

For a complete overview of the numerous attributes supported as well as additional examples, see the reference material in “SELECT and EXCLUDE” on page 884.

The following example in Figure 580 shows part of the result of the standard input member CKRLPROG provided in the SCKRCARL library. It selects PADS data sets using the PADS keyword on the SELECT command combined with restriction to the DATASET class. The SORTLIST command requests a listing of the data set type, volume serial, data set name, universal access, standard access list, and conditional access list for the selected profiles. The sort order is defined by the order of the field names. In this example, the fields are data set name (`dsn`), volume serial (`volser`), and data set type (`dstype`).

```
Include CKRALLOC (ISPF variable)
     2 |/* Data for CKRLPROG */
     3 |alloc type=UNLOAD dsn='SYSAPPL.CNRACF.DD971028.UNLOAD'  complex=DD971028
     4 |
     6 |alloc type=CKFREEZE dsn='SYSAPPL.CNRACF.DD971028.CKFREEZE'  complex=DD971028
     7 |
     8 |alloc type=CKRCMD DD=CKR2CMD
End of  CKRALLOC (include level 1)

Include CKRCMDV  (ISPF variable)
     1 |I DD=CKR2CRL M=CKRLPROG

Include CKR2CRL  C##A.D.C2RNEW.SCKRCARL(CKRLPROG)                       SM3005
     1 | /*************************************************BeginModule********
     2* | * LICENSED MATERIALS - PROPERTY OF IBM
     3* | * 5655-T01
     4* | * Copyright IBM Corp. 1989, 2011
     5* | * All Rights Reserved
     6* | * US Government Users Restricted Rights - Use, duplication or
     7* | * disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
     8* | * File-stamp: <020404 MR 11:37:08 CKRLPROG.SCKRCARL>
     9* | * FMID: HCKR1C0 RMID: HCKR1C0 IBM Security zSecure Base 1.13.0
    10* | * Purpose:
    11* | *     Program Profile Overview
    12* | *     Program Accessed Dataset Overview
    13* | * History:
    14* | ***************************************************EndModule********/
    15 |newlist title='Program profile overview'
    16 |   select   class=program segment=base
    17 |   sortlist key(nondispl) | complex key(8) memlst(sort) uacc(3),
    18 |                    acl(sort,43) acl:pgmrname
    19 |
    20 |newlist title='Program Accessed Dataset overview'
    21 |   select   pads class=dataset segment=base
    22 |   sortlist hexkey(nondispl) | complex key(36,wrap) volser dstype uacc,
    23 |                          acl(sort,43) acl:pgmrname
    24 |
End of  CKR2CRL  (include level 2)

End of  CKRCMDV  (include level 1)
```

Figure 580. Sample output of CARLa script CKRLPROG PADS report - Part 1

```
P R O F I L E   L I S T I N G   28 Oct 1997 00:05                                                    page    4
Program Accessed Dataset overview

Complex  Profile key                          Volume DsTyp UACC    User     Access  ACL id   When            Name
DD971028 C##A.X.RC921204.**                            NONE    -group-  READ    C##ARACF PROGRAM  CNARACF
                                                               -group-  READ    C##ARACF PROGRAM  CNAUDIT
                                                               -group-  READ    C##ARACF PROGRAM  CNAUDITS
                                                               -group-  READ    C##ARACF PROGRAM  CNAUDIT2
                                                               -group-  READ    C##ARACF PROGRAM  CNRACF
                                                               -group-  READ    C##BRACF PROGRAM  CNARACF
                                                               -group-  READ    C##BRACF PROGRAM  CNAUDIT
                                                               -group-  READ    C##BRACF PROGRAM  CNAUDITS
                                                               -group-  READ    C##BRACF PROGRAM  CNAUDIT2
                                                               -group-  READ    C##BRACF PROGRAM  CNRACF
                                                               -group-  READ    C##C
DD971028 C##AINT.RACFTEST.CONDACL.*                    NONE    -group-  READ    C##A     CONSOLE  CRMAINT
                                                               -group-  READ    C##A     CONSOLE  CRMASCH
                                                               -group-  READ    C##A     CONSOLE  SDSF
DD971028 C##BER2.CNRACF.SYSPRINT              SME003   NONE    C##BERT  READ    C##BERT  PROGRAM  TESTPADS BERT LINEKER
DD971028 DFHSM.BACK.T293502.CRMBER2.CNRACF.I7 MIGRAT   NONE    C##BERT  READ    C##BERT  PROGRAM  TESTPADS BERT LINEKER
         287
DD971028 SYSAPPL.CNRACF.BACK1DAY.**                    NONE    -group-  READ    C##ACONF
                                                               -group-  READ    C##ARACF
                                                               -group-  READ    C##BRACF
                                                               -group-  READ    C##BREAD
                                                               -group-  READ    C##GRACF PROGRAM  CNARACF
                                                               -group-  READ    C##GRACF PROGRAM  CNARACF2
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDIT
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDITS
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDIT2
                                                               -group-  READ    C##GRACF PROGRAM  CNRACF
                                                               -group-  READ    C##GRACF PROGRAM  CNRAUDIT
                                                               -group-  ALTER   SYSAPPL
                                                               -group-  ALTER   SYSPROG
                                                               C##BJTI  READ    C##BJTI                    JAMES T. ISAACS
                                                               C##BJT2  READ    C##BJT2                    JAMES T. ISAACS
                                                               C##BNAT  READ    C##BNAT                    NATE A. TAILOR
                                                               C##BNA2  READ    C##BNA2                    NATE A. TAILOR
                                                               C##BUIT  READ    C##BUIT                    ULRIC I. TERWILLIGER
                                                               C##CUST  READ    C##CUST                    ZSECUR DEMO ACCOUNT
                                                               R##PROB  ALTER   R##PROB                    ROBERT BERNARD
DD971028 SYSAPPL.CNRACF.**                             NONE    -group-  READ    C##ACONF
                                                               -group-  READ    C##ARACF
                                                               -group-  READ    C##BRACF
                                                               -group-  READ    C##CDEMO
                                                               -group-  READ    C##GRACF PROGRAM  CNARACF
                                                               -group-  READ    C##GRACF PROGRAM  CNARACF2
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDIT
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDITS
                                                               -group-  READ    C##GRACF PROGRAM  CNAUDIT2
                                                               -group-  READ    C##GRACF PROGRAM  CNRACF
                                                               -group-  READ    C##GRACF PROGRAM  CNRAUDIT
                                                               -group-  ALTER   SYSAPPL
                                                               -group-  ALTER   SYSPROG
                                                               C##BJTI  READ    C##BJTI                    JAMES T. ISAACS
                                                               C##BJT2  READ    C##BJT2                    JAMES T. ISAACS
```

Figure 581. Sample output of CARLa script CKRLPROG PADS report - Part 2

Finding all occurrences of a string

You can use the following CARLa commands to run a quick scan of the entire RACF database for a specified string:

```
SELECT SCAN=string
SORTLIST CLASS, KEY
```

These commands produce output like the output shown in Figure 582 on page 1687.

```
P R O F I L E   L I S T I N G   28 Oct 1997 00:05                    page 1

Class    Profile key
DATASET  C##A.D.CNFJTI.**
DATASET  C##A.D.CNRJTI.**
DATASET  C##A.D.CNRNEW.CNRCLIB
DATASET  C##A.D.CNRNEW.CNRMLIB
DATASET  C##A.D.CNRNEW.CNRPLIB
DATASET  C##A.D.CNRNEW.CNRSAMP
DATASET  C##A.L.**
DATASET  C##BJTI.**
DATASET  C##BJT2.**
DATASET  SYSAPPL.CNRACF.**
DATASET  SYSAPPL.CNRACF.BACK1DAY.**
FACILITY $CNG.CMD.LIST
FACILITY $CNG.SCP.G.CR.CRM.CRMQ.**.CRMBQAMC
FACILITY $CNG.SCP.ID.CRMBQAMC.**
GROUP    C##B
GROUP    C##BREAD
GROUP    C##CNG
GROUP    C##GRACF
USER     C##BJT2
USER     C##BJT2
```

Figure 582. Sample SORTLIST output with SELECT SCAN=

The SCAN parameter scans all of the fields in each profile. To limit the scan to a particular field, the FIELD parameter can be specified on the SELECT command as shown in the following example:

```
SELECT CLASS=DATASET FIELD=INSTDATA SCAN=string
SORTLIST CLASS KEY INSTDATA
```

These commands search for *string* in the installation data of DATASET profiles. This search can also be performed using the following commands:

```
SELECT CLASS=DATASET INSTDATA=:string
SORTLIST CLASS KEY INSTDATA
```

USRDATA - Reporting on user fields

The USR field is a rather special case in zSecure, somewhat like the ACL field. The USR field is a combination field containing the *user fields*USRNM, USRFLG, and USRDATA. These fields cannot be set or listed using normal RACF commands, but they are used by IBM and third-party developers to store information in RACF profiles. The CKGRACF authorized component of zSecure provides access to the user fields in most profile types and also uses these fields to store CKGRACF-specific settings. The USR field, its use in zSecure, and the CKGRACF-specifics, are described in detail "User fields." For more information of the CKGRACF authorized component, see "Auditing CKGRACF" on page 371.

User fields

The following example shows how to display information stored in user fields in the USER class by using the following commands:

```
select class=user usrcnt>0
sortlist class key(8) usrcnt usrnm usrflg usrdata usr("Combination field")
```

The following report contains information that includes phone/fax numbers, email addresses, and CKGRACF data. Both the USRNM, USRFLG and USRDATA fields and the USR combination field are listed. The USR field has special support to interpret CKGRACF data.

```
P R O F I L E   L I S T I N G   28 Oct 1997 00:05                                    page 1

Class    Profile  #Usrf UsrField Fl User data                          Combination field
USER     C##BGUS      3 PHONE    00 BLAH                              PHONE    00 BLAH
                         TELEFAX  00 +31 15 2628070                    TELEFAX  00 +31 15 2628070
                         TELEFOON 00 +31 15 2618821                    TELEFOON 00 +31 15 2618821
USER     C##BGU3      4 CNGSCHED 00 .p.|.p.|GRPADMIN.C##BGUS .*M..p.|.     Scheduled event: Schedule 'GRPADMIN' disable 14
                         CNGSCHED 00 .....p.ñGRPADMIN.C##BGUS .*M..p.|.     Scheduled event: Schedule 'GRPADMIN' enable 19 M
                         CNGSCHED 00 .p.¾.p.¾SYSADMIN.C##BGUS .*¤..p.|.     Scheduled event: Schedule 'SYSADMIN' disable 15
                         CNGSCHED 00 .....p..SYSADMIN.C##BGUS .*¤..p.|.     Scheduled event: Schedule 'SYSADMIN' enable 23 M
USER     C##BMCO      2 CNGAUTH  00 .C##BMC2 . ˙.m.p.|                     Authority setting SINGLE set by C##BMC2 at  3 Ju
                         PHONE    00 0104270326                          PHONE    00 0104270326
USER     C##QA005     5 CNGAUTH  00 .C##QARUN.?[¹.p..                     Authority setting DUAL set by C##QARUN at  7 Oct
                         CNGQUEUE 85 .p.ñ..USER C##QA005 SCHEDULE QA#UIT DIS Queued command (CA): USER C##QA005 SCHEDULE QA#U
                         CNGQUEUE 85 .p.ñ..USER C##QA005 SCHEDULE QA#UIT ENA Queued command (CA): USER C##QA005 SCHEDULE QA#U
                         CNGSCHED 00 .p...p..QA#UIT  .C##QA1G .M...p...     Scheduled event: Schedule 'QA#UIT' disable  7 Oc
                         CNGSCHED 00 .....p..QA#UIT  .C##QA1G .M...p...     Scheduled event: Schedule 'QA#UIT' enable  8 Oct
USER     C##QA015     1 CNGDFLT  00 .O.³3N1.C##QARUN..LP.p..               Default password set by C##QARUN at 20 Sep 1997
USER     R##SLIN      1 PHONE    00 015 2622722 - 233                     PHONE    00 015 2622722 - 233
USER     R##PTST      2 TELEFAX  00 +31 15 2628070                        TELEFAX  00 +31 15 2628070
                         TELEFOON 00 +31 15 2618821                    TELEFOON 00 +31 15 2618821
USER     TEMPTEST     1 CNGDFLT  00 Ù.EOvA°wC##BERT .r-..p..              Default password set by C##BERT at 11 May 1997 1
```

Figure 583. Sample LIST output user-fields

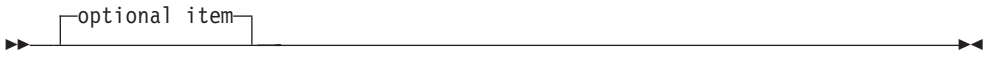
Appendix A. Reading Syntax Diagrams

The following rules apply to the syntax diagrams used in this manual:

- Read the syntax diagrams from left to right, from top to bottom, following the path of the line.
  - The ▸▸— symbol indicates the beginning of a statement.
  - The —▸ symbol indicates that the statement syntax is continued on the next line.
  - The ▸— symbol indicates that a statement is continued from the previous line.
  - The —▸◂ symbol indicates the end of a statement.
  - Diagrams of syntactical units other than complete statements start with the ▸— symbol and end with the —▸ symbol.
- Required items appear on the horizontal line (the main path).

- Optional items appear below the main path.

- If an optional item appears above the main path, that item has no effect on the execution of the statement and is used only for readability.

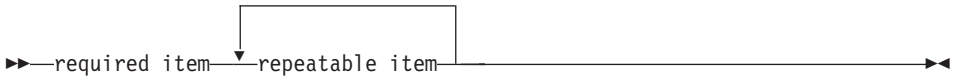


- If you can choose from two or more items, they appear vertically, in a stack.
  - If you must choose one of the items, one item of the stack appears on the main path.

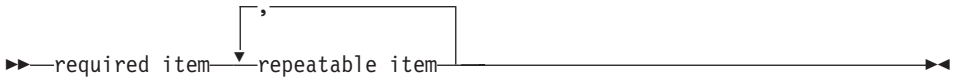
  - If choosing one of the items is optional, the entire stack appears below the main path.

  - If one of the items is the default, it appears above the main path and the remaining choices are shown below.

- An arrow returning to the left, above the main line, indicates an item that can be repeated.
  - If the repeat arrow does not include any characters, you must separate repeated items with a space.



  - If the repeat arrow contains a comma, you must separate repeated items with a comma.



  - A repeat arrow above a stack indicates that you can repeat the items in the stack.
- Keywords appear in uppercase (for example, **USER**). They must be spelled exactly as shown. Variables appear in all lowercase letters (for example, *userid*). They represent user-supplied names or values.
- If punctuation marks, parentheses, arithmetic operators, or other such symbols are shown, you must enter them as part of the syntax.

Appendix B. Support information

This section describes the following options for obtaining support for IBM products:

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. Learn how to optimize your results by using available resources, support tools, and search methods and how to receive automatic updates.

Available technical resources

In addition to the Security zSecure information center, you can access the following technical resources to help you answer questions and resolve problems:

- Access the Tivoli support site to view technotes, APARs (problem reports) and other related information at http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivolizSecureSuite.html
- Access the Redbooks Domain to locate current redbooks for Security zSecure at http://www.redbooks.ibm.com/
- Access Tivoli support forums and communities at http://www-01.ibm.com/software/sysmgmt/products/support/Tivoli_Communities.html

Searching with support tools

The following tools are available to help you search IBM knowledge bases:

- **IBM Support Assistant** (ISA) is a free software serviceability workbench that helps you resolve questions and problems with IBM software products. Instructions for downloading and installing the ISA can be found on the ISA website: http://www.ibm.com/software/support/isa.
- **IBM Software Support Toolbar** is a browser plug-in that provides you with a mechanism to easily search IBM support sites. You can download the toolbar at http://www.ibm.com/software/support/toolbar/.

Searching tips

The following resources describe how to optimize your search results:

- Searching the IBM Support website: http://www-01.ibm.com/support/us/srchtips.html
- Using the Google search engine:http://www.google.com/support/

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your Tivoli software product, follow these steps:

1. Go to the IBM Software Support website at http://www.ibm.com/software/support.
2. Under **Select a brand and/or product**, select **Tivoli**.
3. Click the right arrow to view the Tivoli support page.
4. Use the **Select a category** field to select the product.
5. Select your product and click the right arrow that shows the **Go** hover text.
6. Under **Download**, click the name of a fix to read its description and, optionally, to download it.

   If there is no **Download** heading for your product, supply a search term, error code, or APAR number in the field provided under **Search Support (this product)**, and click the right arrow that shows the **Go** hover text.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

1. Go to the IBM Software Support website at http://www.ibm.com/software/support.
2. Click **My support** in the far upper right corner of the page under **Personalized support**.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. The **Edit profile** tab is displayed.
5. In the first list under **Products**, select **Software**. In the second list, select a product category (for example, **Systems and Asset Management**). In the third list, select a product sub-category (for example, **Application Performance & Availability** or **Systems Performance**). A list of applicable products is displayed.
6. Select the products for which you want to receive updates.
7. Click **Add products**.
8. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
9. In the **Documents** list, select **Software**.
10. Select **Please send these documents by weekly email**.
11. Update your e-mail address as needed.
12. Select the types of documents you want to receive.
13. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
Call 1-800-IBM-4You (1-800-426-4968).

Registering with IBM Software Support

Before you can receive weekly e-mail updates about fixes and other news about IBM products, you need to register with IBM Software Support. To register with IBM Software Support, follow these steps:

1. Go to the IBM Software Support site at the following Web address:

   http://www.ibm.com/software/support
2. Click **Register** in the upper right corner of the support page to establish your user ID and password.
3. Complete the form, and click **Submit**.

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational® products, and DB2 and WebSphere® products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online
  Go to the Passport Advantage website at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm .

  By phone
  For the phone number to call in your country, go to the IBM Software Support website at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request website at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink, CATIA, Linux, OS/390, iSeries®, pSeries®, zSeries, and other support agreements, go to the IBM Support Line website at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage website at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at

http://www14.software.ibm.com/webapp/set2/sas/f/handbook/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information"
3. "Submitting problems"

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Use the following criteria to understand and assess the business impact of the problem that you are reporting:

Severity 1
The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4
The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- Which software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online
Click **Submit and track problems** on the IBM Software Support site at http://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone
For the phone number to call in your country, go to the contacts page of the

IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix C. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

Special characters

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Printed in USA

LC14-7663-00